TP-LINK®

User Guide

TL-R860
Cable/DSL Router

Ver:1.0

COPYRIGHT & TRADEMARKS

Specifications are subject to change without notice. TP-LINK® is a registered trademark of TP-LINK Technologies Co., Ltd. Other brands and product names are trademarks or registered trademarks of their respective holders.

No part of the specifications may be reproduced in any form or by any means or used to make any derivative such as translation, transformation, or adaptation without permission from TP-LINK Technologies Co., Ltd. Copyright © 2007 TP-LINK Technologies Co., Ltd. All rights reserved.

FCC STATEMENT

This equipment has been tested and found to comply with the limits for a Class B digital device, pursuant to part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation. This equipment generates, uses and can radiate radio frequency energy and, if not installed and used in accordance with the instructions, may cause harmful interference to radio communications. However, there is no guarantee that interference will not occur in a particular installation. If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one or more of the following measures:

- Reorient or relocate the receiving antenna.
- Increase the separation between the equipment and receiver.
- Connect the equipment into an outlet on a circuit different from that to which the receiver is connected.
- Consult the dealer or an experienced radio/ TV technician for help.

This device complies with part 15 of the FCC Rules. Operation is subject to the following two conditions:

1) This device may not cause harmful interference.

This device must accept any interference received, including interference that may cause undesired operation.

CE Mark Warning

This is a class B product. In a domestic environment, this product may cause radio interference, in which case the user may be required to take adequate measures.

SAFETY NOTICES

Caution: Do not use this product near water, for example, in a wet basement or near a swimming pool.

Avoid using this product during an electrical storm. There may be a remote risk of electric shock from lightning.

COMMENT

Package contents 1

Chapter 1. About this Guide 2

1.1 Purposes 2

1.2 Conventions 2

1.3 Overview of this User Guide 2

Chapter 2. Introduction 3

2.1 Overview of the Router 3

2.2 Features 3

2.3 Panel Layout 4

2.3.1 The Front Panel 4

2.3.2 The Rear Panel 4

Chapter 3. Connecting the Router 6

3.1 System Requirements 6

3.2 Installation Environment Requirements 6

3.3 Connecting the Router 6

Chapter 4. Quick Installation Guide 8

4.1 TCP/IP configuration 8

4.2 Quick Installation Guide 9

Chapter 5. Configuring the Router 13

5.1 login 13

5.2 Status 13

5.3 Quick Setup 14

5.4 Network 14

5.4.1 LAN 14

5.4.2 WAN 15

5.4.3 MAC Clone 20

5.5 DHCP 21

5.5.1 DHCP Settings 21

5.5.2 DHCP Clients List 22

5.5.3 Address Reservation 22

5.6 Forwarding 24

5.6.1 Virtual Servers 24

5.6.2 Port Triggering 25

5.6.3 DMZ 27

5.6.4 UPnP 28

5.7 Security 29

5.7.1 Firewall 29

5.7.2 IP Address Filtering 30
5.7.3 Domain Filtering 32
5.7.4 MAC Filtering 33
5.7.5 Remote Management 34
5.7.6 Advanced Security 35
5.8 Static Routing 37
5.9 IP & MAC Binding Setting 39
5.9.1 Binding Setting 39
5.9.2 ARP List 40
5.10 DDNS 41
5.10.1 Dyndns.org DDNS 41
5.10.2 Oray.net DDNS 42
5.10.3 Comexe.cn DDNS 43
5.11 System Tools 44
5.11.1 Time 44
5.11.2 Firmware 45
5.11.3 Factory Defaults 46
5.11.4 Backup and Restore 46
5.11.5 Reboot 46
5.11.6 Password 47
5.11.7 Log 48
5.11.8 Statistics 48

Appendix A: FAQ 50

Appendix B: Configuring the PCs 54

Appendix C: Specifications 58

Appendix D: Glossary 59

Appendix E: Contact Information 60

Package contents

The following contents should be found in your box:

- One TL-R860 Cable/DSL Router
- One AC power Adapter for TL-R860 Cable/DSL Router
- Quick Installation Guide
- One Resource CD for TL-R860 Cable/DSL Router, including:
  - This Guide
  - Other Helpful Information

Note: If any of the listed contents are damaged or missing, please contact the retailer from whom you purchased the TL-R860 Cable/DSL Router for assistance.

Chapter 1. About this Guide

Thank you for choosing the TL-R860 Cable/DSL Router. This router provides dedicated solutions for Small Office/Home Office (SOHO) networks. With your network all connected, your local network can share Internet access, files and fun for multiple PCs through one ISP account.

It is an easy, web-based setup for installation and management. Even though you may not be familiar with the router, this guide will make configuring the router easy. Before installing the router, please look through this guide to get to know all the router's functions.

1.1 Purposes

This Guide tells you how to use the TL-R860 Cable/DSL Router.

1.2 Conventions

The router mentioned in this guide stands for TL-R860 Cable/DSL Router.

1.3 Overview of this User Guide

Chapter 1: About this Guide
Chapter 2: Introduction
Chapter 3: Connecting the Router
Chapter 4: Quick Installation Guide
Chapter 5: Configuring the Router
Appendix A: FAQ
Appendix B: Configuring the PCs
Appendix C: Specifications
Appendix D: Glossary
Appendix E: Contact Information

Chapter 2. Introduction

2.1 Overview of the Router

The TL-R860 Cable/DSL Router integrates an 8-port switch, firewall, and NAT-router. Its design is dedicated to Small Office/Home Office (SOHO) network solutions. The TL-R860 Cable/DSL Router will allow you to connect your network better than ever, sharing Internet Access, files and fun, easily and securely.

The TL-R860 Cable/DSL Router provides flexible access control so that parents or network administrators can establish restricted access policies for children or staff. It has built-in NAT and DHCP server supporting static IP address distributing. It supports Virtual Server and DMZ host for Port Triggering needs, and remote management and log so that network administrators can manage and monitor the network on real time. It also supports VPN pass-through for sensitive data secure transmission.

The TL-R860 Cable/DSL Router is easy-to-manage. Quick Setup is supported and friendly help messages are provided for every step. So you can configure it quickly and share Internet access, files and fun comfortably.

2.2 Features

- Complies with IEEE802.3, IEEE802.3u standards
- Built in 8-port 10/100Mbps switch
- Ethernet connection to a WAN device, such as a Cable modem or DSL modem
- Shares data and Internet access for the network, connecting Internet through PPPoE on demand and disconnecting when idle
- Built-in NAT and DHCP server supporting static IP address distributing
- Supports Virtual Server, Port Triggering, and DMZ host
- Built-in firewall supporting IP address filtering, Domain Name filtering, and MAC address filtering
- Supports connecting/disconnecting Internet at a specified time of day
- Supports access control, allowing parents and network administrators to establish restricted access policies based on the time of day for children or staff
- Supports TCP/IP, PPPoE, DHCP, ICMP, NAT, SNTP
- Supports UPnP, Dynamic DNS, Static Routing, VPN pass-through
- Supports Traffic Statistics
- Supports ICMP-FLOOD, UDP-FLOOD, TCP-SYN-FLOOD filter
- Ignores Ping packets from WAN or LAN ports
- Supports firmware upgrade
- Supports Remote and Web management

2.3 Panel Layout

2.3.1 The Front Panel

The front panel of the TL-R860 consists of several LED indicators, which is designed to indicate connections. Viewed from left to right. Table 2-1 describes the LEDs on the front panel of the router.

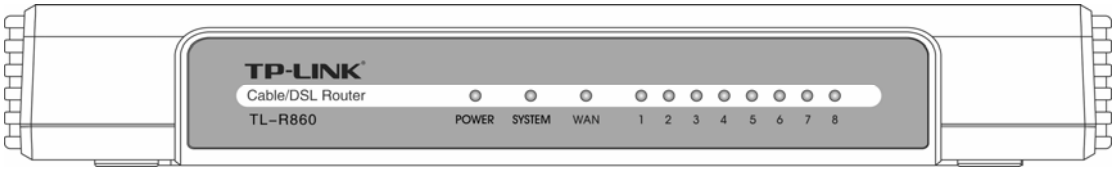


Figure 2-1 Front Panel sketch

Name	Action	Description
Power	Not lit	No power
	Lit up	Power on
System	Not lit	The Router has an error
	Lit up	The Router has an error
	Flashing	The router works properly
Link/Act	Not lit	There is no device linked to the corresponding port
	Lit up	There is a device linked to the corresponding port but no activity
	Flashing	There is an active device linked to the corresponding port

Table 2-1 The LEDs description

2.3.2 The Rear Panel

The rear panel contains the following features. (Viewed from left to right:)

- Factory Default Reset button

  There are two ways to reset the router's factory defaults:

  1. Use the **Factory Defaults** function on **System Tools** -> **Factory Defaults** page in the router's Web-based Utility.
  2. Use the Factory Default Reset button: First, turn off the router's power. Second, press the default reset button, then turn on the router's power, and hold the reset button about 3 seconds until the System LED flashes for three times. Finally, release the reset button and wait for the router to reboot.

  Note: Ensure the router is powered on before it restarts completely.
- WAN RJ45 port for connecting the router to a cable, DSL modem or Ethernet
- Eight LAN 10/100Mbps RJ45 ports for connecting the router to the local PCs
- AC power socket: only use the power adapter supplied with the TL-R860 Cable/DSL Router, use of a different adapter may result in product damage.

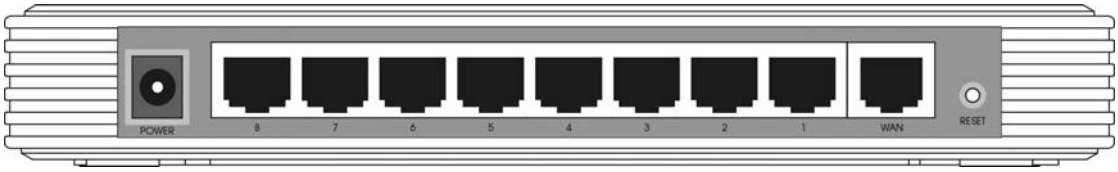


Figure 2-2 Rear Panel sketch

Chapter 3. Connecting the Router

3.1 System Requirements

- Broadband Internet Access Service (DSL/Cable/Ethernet)
- One DSL/Cable modem that has an RJ45 connector (It's not necessary if you connect the router to Ethernet)
- Each PC on the LAN needs a working Ethernet Adapter and an Ethernet cable with RJ45 connectors
- TCP/IP protocol must be installed on each PC
- Web browser, such as Microsoft Internet Explorer 5.0 or later, Netscape Navigator 6.0 or later

3.2 Installation Environment Requirements

- Not in direct sunlight or near a heater or heating vent
- Not cluttered or crowded. There should be at least 2 inches (5 cm) of clear space on all sides of the router
- Well ventilated (especially if it is in a closet)
- Operating temperature: 0℃~40℃ (32℉~104℉)
- Operating Humidity: 10%~90%RH, Non-condensing

3.3 Connecting the Router

Before you install the router, you should connect your PC to the Internet through your broadband service successfully. If there is any problem, please contact with your ISP for help. After that, please install the router according to the following steps. Don't forget to pull out the power plug and keep your hands dry.

1. Power off your PC(s), Cable/DSL modem, and the router.
2. Connect the PC(s) and all Switches/Hubs on your LAN to the LAN Ports on the router, shown in Figure 3-1.
3. Connect the DSL/Cable modem to the WAN port on the router, shown in Figure 3-1.
4. Connect the AC power adapter to the AC power socket on the router, and the other end into an electrical outlet. The router will start to work automatically.
5. Power on your PC(s) and Cable/DSL modem.

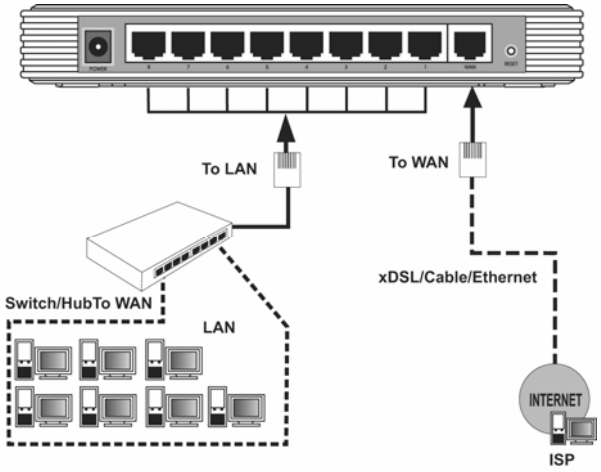


Figure 3-1 Hardware Installation of the TL-R860 Cable/DSL Router

Chapter 4. Quick Installation Guide

After connecting the TL-R860 router into your network, you should configure it. This chapter describes how to configure the basic functions of your TL-R860 Cable/DSL Router. These procedures may take you only a few minutes. You can access the Internet via the router immediately after it has been successfully configured.

4.1 TCP/IP configuration

The default IP address of the TL-R860 Cable/DSL Router is 192.168.1.1, and the default Subnet Mask is 255.255.255.0. These values can be seen from the LAN, and can be changed as your desire. As an example, we use the default values for description in this guide.

Connect the local PCs to the LAN ports on the router. There are then two means to configure the IP address for your PCs.

- Configure the IP address manually
  1) Set up the TCP/IP Protocol for your PC(s).
  2) Configure the network parameters. The IP address is 192.168.1.xxx ("xxx" is from 2 to 254), Subnet Mask is 255.255.255.0, and Gateway is 192.168.1.1 (The router's default IP address).
- Obtain an IP address automatically
  1) Set up the TCP/IP Protocol in "**Obtain an IP address automatically**" mode on your PC(s).
  2) Power off the router and PC(s). Then turn on the router, and restart the PC(s). The built-in DHCP server will assign IP addresses for the PC(s).

Note: If you need instructions as to how to do this, please refer to Appendix B: "Configuring the PCs.".

Now, you can run the Ping command in the **command prompt** to verify the network connection between your PC(s) and the router. The following example is in Windows 2000.

Open a command prompt, and type *ping 192.168.1.1*, then press **Enter**.

```
Pinging 192.168.1.1 with 32 bytes of data:

Reply from 192.168.1.1: bytes=32 time<10ms TTL=64
Reply from 192.168.1.1: bytes=32 time<10ms TTL=64
Reply from 192.168.1.1: bytes=32 time<10ms TTL=64
Reply from 192.168.1.1: bytes=32 time<10ms TTL=64

Ping statistics for 192.168.1.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum =  0ms, Average =  0ms
```

Figure 4-1 Successful result of Ping command

If the result displayed is similar to what is shown in Figure 4-1, the connection between your PC and the router has been established.

```
Pinging 192.168.1.1 with 32 bytes of data:

Request timed out.
Request timed out.
Request timed out.
Request timed out.

Ping statistics for 192.168.1.1:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum =  0ms, Average =  0ms
```

Figure 4-2 Failed result of Ping command

If the result displayed is similar to what is shown in Figure 4-2, it means that your PC has not connected to the router. If so, refer to the following steps for a solution:

1. Is the connection between your PC and the router correct?
   Note: The Link/Act LEDs of LAN port on the router and LEDs on your PC's adapter should be lit.
2. Is the TCP/IP configuration for your PC correct?
   Note: If the router's IP address is 192.168.1.1, your PC's IP address must be within the range of 192.168.1.2 ~ 192.168.1.254, the gateway must be 192.168.1.1

4.2 Quick Installation Guide

With a Web-based (Internet Explorer or Netscape® Navigator) utility, the TL-R860 Cable/DSL Router is easy to configure and manage. The Web-based utility can be used on any Windows, Macintosh or UNIX OS with a web browser.

Connect to the router by typing *http://192.168.1.1* in the address field of web browser.

Figure 4-3 Login to the router

After a moment, a login window will appear similar to that shown in Figure 4-4. Enter **admin** for the User Name and Password, both in lower case letters. Then click the **OK** button or press the **Enter** key.

Figure 4-4 Login Windows

Note: If the above screen does not prompt, it means that your web-browser has been set to a proxy. Go to Tools menu>Internet Options>Connections>LAN Settings, in the screen that appears, cancel the Using Proxy checkbox, and click OK to finish it.

If the User Name and Password are correct, you can configure the router using the web browser. Please click the **Quick Setup** link on the left of the main menu and the Quick Setup screen will appear.

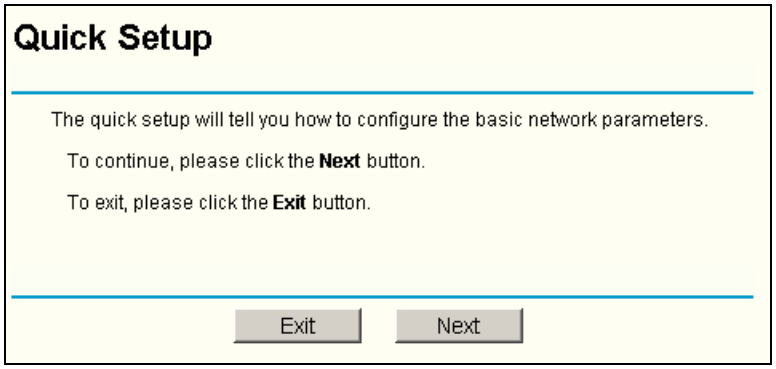

Quick Setup
The quick setup will tell you how to configure the basic network parameters.
To continue, please click the Next button.
To exit, please click the Exit button.
Exit
Next

Figure 4-5 Quick Setup

Click **Next**, the **Choose WAN Connection Type** page will appear, shown in Figure 4-6.

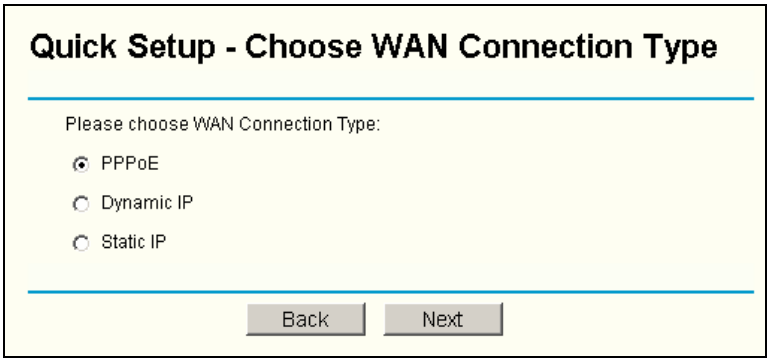


Figure 4-6 Choose WAN Connection Type

The router supports three popular ways to connect to Internet. Please select one compatible with your ISP, if you are given another way not listed here, refer to **Network→ WAN** for detailed list. Click **Next** to enter the necessary network parameters.

If you choose "**PPPoE**", you will see this page shown in Figure 4-7:

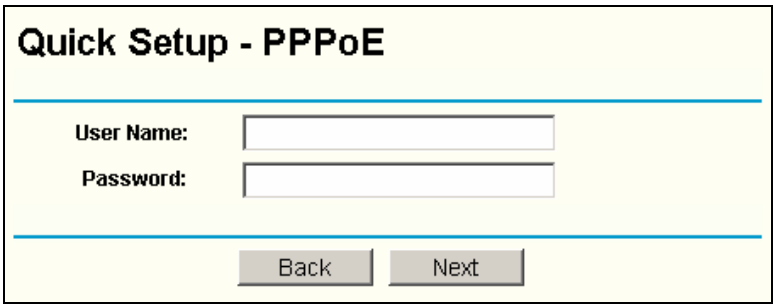


Figure 4-7 Quick Setup - PPPoE

- **User Name and Password -** Enter the **User Name** and **Password** provided by your ISP. These fields are case sensitive. If you have difficulty with this process, please contact your ISP.

If you choose " **Dynamic IP**", the router will automatically receive the IP parameters from your ISP without needing to enter any parameters.

If you Choose "**Static IP**", the Static IP settings page will appear, shown in Figure 4-8:

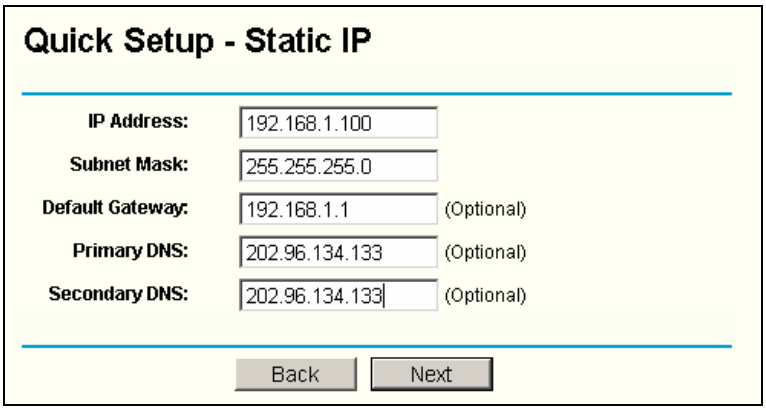


Figure 4-8 Quick Setup - Static IP

Note: The IP parameters should have been provided by your ISP.

- **IP Address -** This is the WAN IP address as seen by external users on the Internet (including your ISP). Enter the IP address into the field.
- **Subnet Mask -** The Subnet Mask is used for the WAN IP address, it is usually 255.255.255.0
- **Default Gateway -** Enter the gateway into the box if required.
- **Primary DNS -** Enter the DNS Server IP address into the boxes if required.
- **Secondary DNS -** If your ISP provides another DNS server, enter it into this field.

Click the **Next** button, then you will see the Finish page:

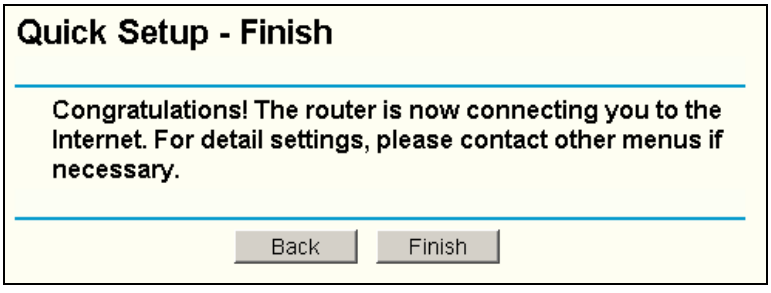

Quick Setup - Finish
Congratulations! The router is now connecting you to the Internet. For detail settings, please contact other menus if necessary.
Back
Finish

Figure 4-9 Quick Setup - Finish

After finishing all configurations of basic network parameters, please click **Finish** button to exit this **Quick Setup**.

Chapter 5. Configuring the Router

This chapter describes each web page's key functions.

5.1 login

After your successful login, you can configure and manage the router. There are nine main menus on the left of the web-based utility. Submenus will be available after you click one of the main menus. The nine main menus are: **Status, Quick Setup, Network, DHCP, Forwarding, Security, Static Routing, DDNS and System Tools.** On the right of the web-based utility, there are the detailed explanations and instructions for the corresponding page. To apply any settings you have altered on the page, please click the **Save** button.

There are the detailed explanations for each web page's key functions below.

5.2 Status

The Status page displays the router's current status and configuration. All information is read-only.

1. **LAN**
   This field displays the current settings or information for the LAN, including the **MAC address, IP address and Subnet Mask**.

2. **WAN**
   These parameters apply to the WAN port of the router, including **MAC address, IP address, Subnet Mask, Default Gateway, DNS server** and **WAN connection type**. If PPPoE is chosen as the WAN connection type, the **Disconnect** button will be shown here while you are accessing the Internet. You can also cut the connection by clicking the button. If you have not connected to the Internet, a **Connect** button will be shown, you can then establish the connection by clicking the button.

3. **Traffic Statistics**
   This field displays the router's traffic statistics.

4. **System Up Time**
   This field displays the time since router is powered on or is rebooted.

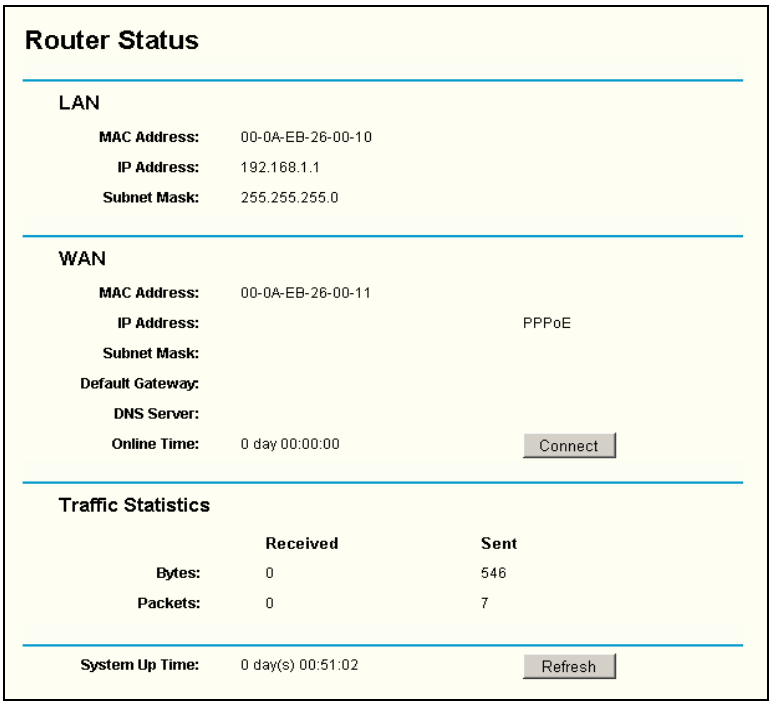


Figure 5-1 Router Status

5.3 Quick Setup

Please refer to Section 4.2: "Quick Installation Guide."

5.4 Network

Figure 5-2 the Network menu

There are three submenus under the Network menu (shown in Figure 5-2): **LAN**, **WAN** and **MAC Clone.** Click any of them, and you will be able to configure the corresponding function. The detailed explanations for each submenu are provided below.

5.4.1 LAN

You can configure the IP parameters of the LAN on this page.

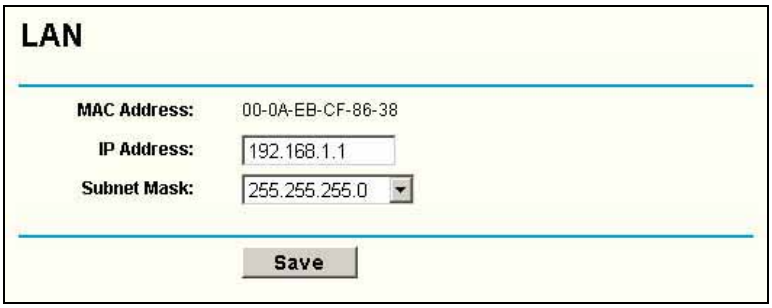


Figure 5-3 LAN

- **MAC Address** - The physical address of the router, as seen from the LAN. The value can't be changed.
- **IP Address -** Enter the IP address of your router (factory default: 192.168.1.1).
- **Subnet Mask -** An address code that determines the size of the network. Normally use 255.255.255.0 as the subnet mask.

Note:

a. If you change the IP address of the LAN, you must use the new IP address to login to the router.

b. If the new LAN IP Address you set is not in the same subnet, the IP address pool in the DHCP sever will not take effect, until they are configured properly.

c. If the new LAN IP Address you set is not in the same subnet, the Virtual Server and DMZ Host may change accordingly at the same time, you'd better re-configure it as well.

5.4.2 WAN

You can configure the WAN port parameters on this page.

First, please choose the WAN Connection Type (Dynamic IP/Static IP/PPPoE/802.1x + Dynamic IP/802.1x + Static IP) to the Internet. The default type is **PPPoE**. If you aren't given any login parameters (fixed IP address, logging ID, etc), please select **Dynamic IP**. If you are given a fixed IP (static IP), please select **Static IP**. If you are given a user name and a password, please select PPPoE. If you are not sure which connection type you use currently, please contact your ISP to obtain the correct information.

1. If you choose **Dynamic IP,** the router will automatically get IP parameters from your ISP. You can see the page as follows (Figure 5-4):

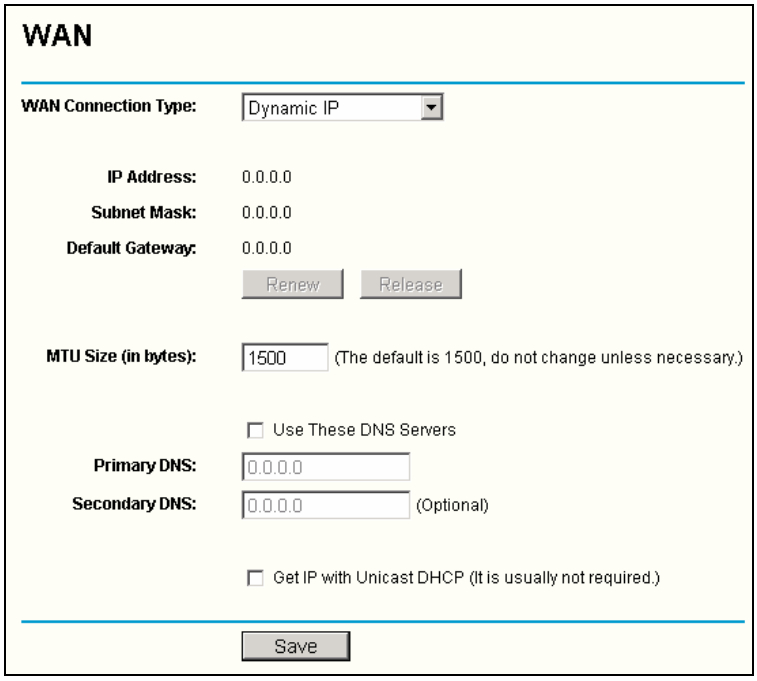


Figure 5-4 WAN - Dynamic IP

This page displays the WAN IP parameters assigned dynamically by your ISP, including IP address, Subnet Mask, Default Gateway, etc. Click the **Renew** button to renew the IP parameters from your ISP. Click the **Release** button to release the IP parameters.

- **MTU Size:** The normal MTU (Maximum Transmission Unit) value for most Ethernet networks is 1500 Bytes. For some ISPs you need to reduce the MTU. But this is rarely required, and should not be done unless you are sure it is necessary for your ISP connection.

  If your ISP gives you one or two DNS addresses, select **Use These DNS Servers** and enter the primary and secondary addresses into the correct fields. Otherwise, the DNS servers will be assigned dynamically from ISP.

- **Note:** If you get 'Address not found' errors when you go to a Web site, it is likely that your DNS servers are set up improperly. You should contact your ISP to get DNS server addresses.
- **Get IP with Unicast DHCP:** A few ISPs' DHCP servers do not support the broadcast applications. If you cannot get the IP address normally, you can choose this option. (You generally need not check this option).

  If you are also given a user name and a password for 802.1x authentication, you should select **802.1x + Dynamic IP** for **WAN Connection Type**, a user name and a password will then appear, shown in Figure 5-5:

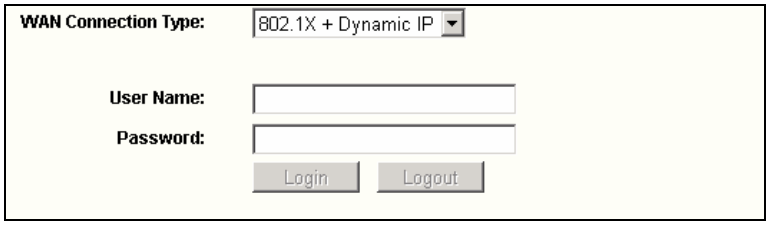


Figure 5-5 WAN - 802.1X + Dynamic IP

- **User Name -** Enter the user name for 802.1x authentication provided by your ISP
- **Password -** Enter the password for 802.1x authentication provided by your ISP.

Click the **Login** button to start 802.1x authentication.

Click the **Logout** button to end 802.1x authentication.

2. If you choose **Static IP,** you should have fixed IP parameters specified by your ISP. The Static IP settings page will appear, shown in Figure 5-6:

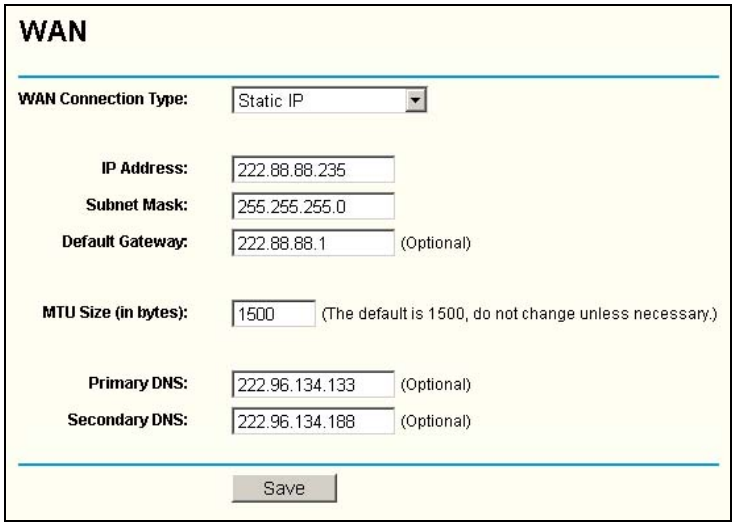


Figure 5-6 WAN - Static IP

You should type the following parameters into the spaces provided:

- **IP Address -** Enter the IP address provided by your ISP.
- **Subnet Mask -** Enter the subnet Mask provided by your ISP, usually is 255.255.255.0.
- **Default Gateway**: (Optional) Enter the gateway IP address provided by your ISP.
- **MTU Size -** The normal MTU (Maximum Transmission Unit) value for most Ethernet networks is 1500 Bytes. For some ISPs you may need to modify the MTU. But this is rarely required, and should not be done unless you are sure it is necessary for your ISP connection.
- **Primary DNS -** (Optional) Type the DNS address provided by your ISP.
- **Secondary DNS -** (Optional) Type another DNS address provided by your ISP if provided.

If you are also given a user name and a password for 802.1x authentication, you should select **802.1x + Static IP** for **WAN Connection Type**, a box will then appear requesting a user name and a password, shown in Figure 5-7:

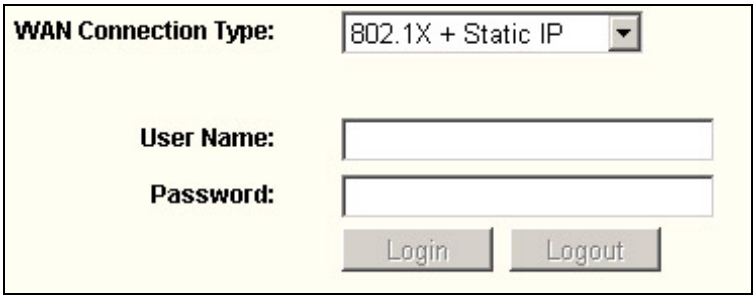


Figure 5-7 WAN - 802.1X + Static IP

- **User Name -** Enter the user name for 802.1x authentication provided by your ISP
- **Password -** Enter the password for 802.1x authentication provided by your ISP.

Click **Login** to start 802.1x authentication.

Click **Logout** to end 802.1x authentication.

3. If you choose **PPPoE,** you should enter the following parameters (Figure 5-8):

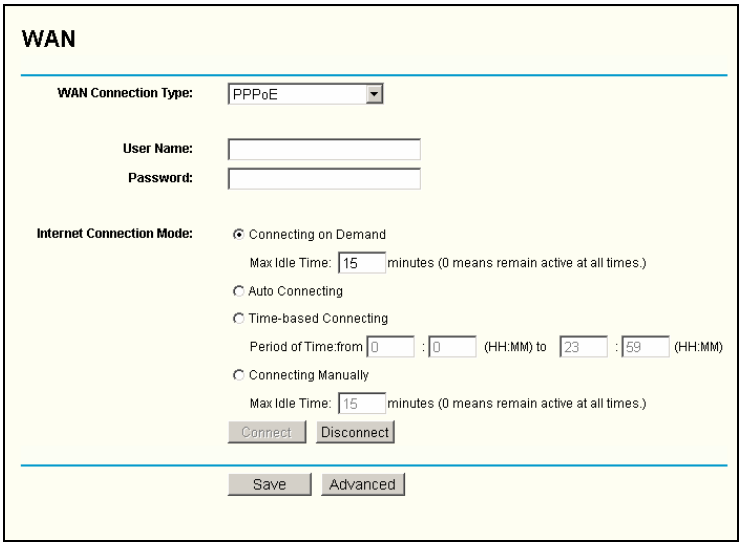


Figure 5-8 WAN - PPPoE

- **User Name/Password -** Enter the User Name and Password provided by your ISP. These fields are case-sensitive.
- **Connect on Demand -** You can configure the router to disconnect your Internet connection after a specified period of inactivity (**Max Idle Time**). If your Internet connection has been terminated due to inactivity, **Connect on Demand** enables the router to automatically re-establish your connection as soon as you attempt to access the Internet again. If you wish to activate **Connect on Demand**, click the radio button. If you want your Internet connection to remain active at all times, enter 0 in the **Max Idle Time** field. Otherwise, enter the number of minutes you want to have elapsed before your Internet connection terminates.

  Caution: Sometimes the connection cannot be disconnected although you specify a time to Max Idle Time. This is because there may still be active applications in the background, which may cause fee accounted by your ISP.
- **Connect Automatically -** Connect automatically after the router is disconnected. To use this option, click the radio button.
- **Time-based Connecting -** You can configure the router to make it connect or

disconnect based on time. Enter the start time in HH:MM for connecting and end time in HH:MM for disconnecting in the **Period of Time** fields.

Note: Only you have set the system time on **System Tools -> Time** page, will the **Time-based Connecting** function take effect.

- **Connect Manually -** You can configure the router to make it connect or disconnect manually. After a specified period of inactivity (**Max Idle Time**), the router will disconnect your Internet connection, and not be able to re-establish your connection automatically as soon as you attempt to access the Internet again. To use this option, click the radio button. If you want your Internet connection to remain active at all times, enter 0 in the **Max Idle Time** field. Otherwise, enter the number in minutes that you wish to have the Internet connecting last unless a new link is requested.

  Caution: Sometimes the connection cannot be disconnected although you specify a time to Max Idle Time. This is because there may still be active applications in the background, which may cause fee accounted by your ISP.

  Click the **Connect** button to connect immediately, Click the **Disconnect** button to disconnect immediately.

Click the **Advanced Settings** button to set up the advanced option, the page shown in Figure 5-9:

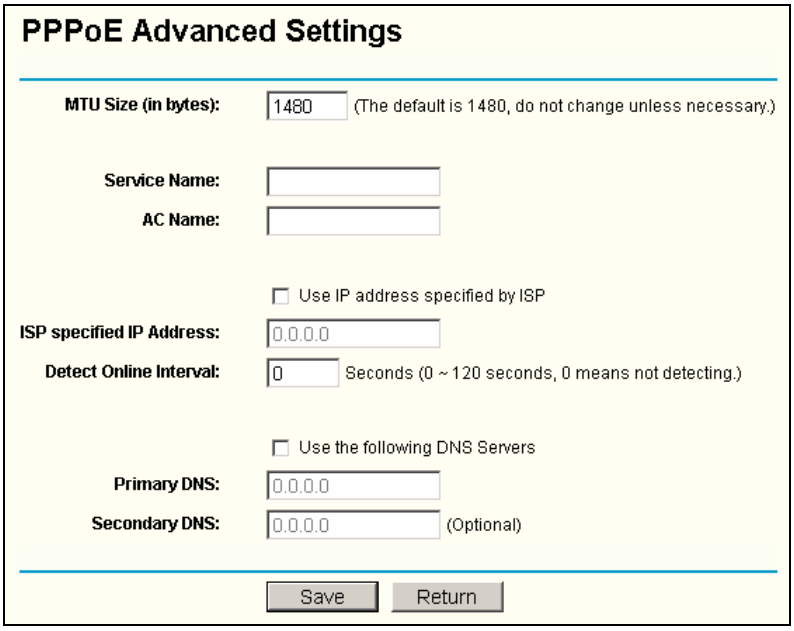


Figure 5-9 PPPoE Advanced Settings

- **Packet MTU -** The default MTU size is 1480 bytes, which is usually fine. For some ISPs, you need modify the MTU. This should not be done unless you are sure it is necessary for your ISP.
- **Service Name/AC Name -** The service name and AC (Access Concentrator) name, this should not be done unless you are sure it is necessary for your ISP.
- **ISP Specified IP Address -** If you know that your ISP does not automatically transmit your IP address to the router during login, click "**Use the IP Address specified by ISP**" check box and enter the IP address , which your ISP provided.
- **Detect Online Interval -** The default value is 0, you can input the value between 0 and 120. The router will detect Access Concentrator online at every interval between

seconds. If the value is 0, it means do not detect.

- **DNS IP Address -** If you know that your ISP does not automatically transmit DNS addresses to the router during login, click "**Use the following DNS servers**" checkbox and enter the IP address of your ISP's primary DNS server. If a secondary DNS server address is available, enter it as well.

Click the **Save** button to save your settings.

5.4.3 MAC Clone

You can configure the MAC address of the WAN port on this page, Figure 5-10:

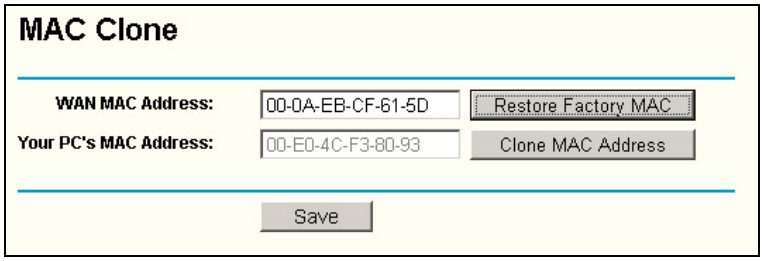


Figure 5-10 MAC Address Clone

Some ISPs require that you register the MAC address of your adapter, which is connected to your cable, DSL modem or Ethernet during installation. You do not generally need to change anything here.

- **WAN MAC Address -** This field displays the current MAC address of the WAN port, which is used for the WAN port. If your ISP requires that you register the MAC address, please enter the correct MAC address into this field. The format for the MAC address is XX-XX-XX-XX-XX-XX (X is any hexadecimal digit).
- **Your PC's MAC Address -** This field displays the MAC address of the PC that is managing the router. If the MAC address is required, you can click the **Clone MAC Address** button and this MAC address will fill in the **WAN MAC Address** field.

Click **Restore Factory MAC** to restore the MAC address of WAN port to the factory default value.

Click the **Save** button to save your settings.

Note:

1) Only the PC(s) on your LAN can use the **MAC Address Clone** feature.
2) If you click the **Save** button, the router will prompt you to reboot.

5.5 DHCP

Figure 5-11 the DHCP menu

There are three submenus under the DHCP menu (shown in Figure 5-11): **DHCP Settings**, **DHCP Clients List** and **Address Reservation.** Click any of them, and you will be able to configure the corresponding function. The detailed explanations for each submenu are provided below.

5.5.1 DHCP Settings

The router is set up by default as a DHCP (Dynamic Host Configuration Protocol) server, which provides the TCP/IP configuration for all the PCs that are connected to the router on the LAN. The DHCP Server can be configured on the page (shown in Figure 5-12):

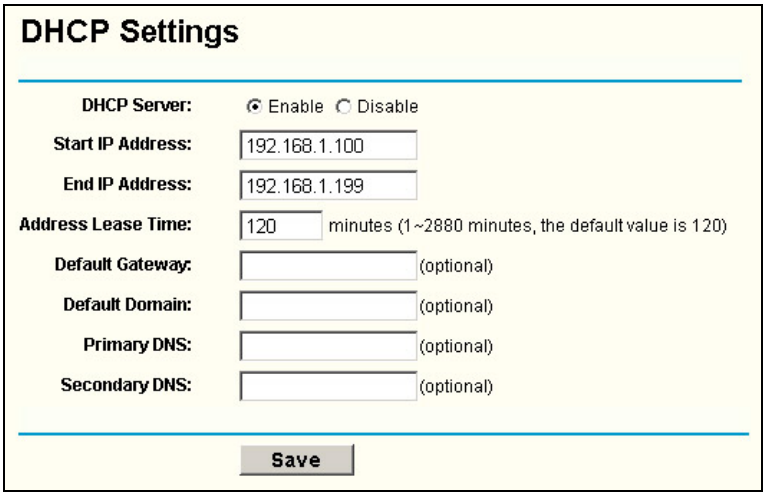


Figure 5-12 DHCP Settings

- **DHCP Server - Enable** or **Disable** the DHCP server. If you disable the Server, you must have another DHCP server within your network or else you must manually configure the computer.
- **Start IP Address -** This field specifies the first of the addresses in the IP address pool. 192.168.1.100 is the default start address.
- **End IP Address -** This field specifies the last of the addresses in the IP address pool. 192.168.1.199 is the default end address.
- **Address Lease Time -** The **Address Lease Time** is the amount of time a network user will be allowed connection to the router with their current dynamic IP address. Enter the amount of time, in minutes, which the user will be "leased" this dynamic IP address. The range of the time is 1 ~ 2880 minutes. The default value is 120 minutes.
- **Default Gateway -** (Optional.) Suggest to input the IP address of the LAN port of

the router, default value is 192.168.1.1

- **Default Domain -** (Optional.) Input the domain name of your network.
- **Primary DNS -** (Optional.) Input the DNS IP address provided by your ISP. Or consult your ISP.
- **Secondary DNS -** (Optional.) Input the IP address of another DNS server if your ISP provides two DNS servers.

Note: To use the DHCP server function of the router, you must configure all computers on the LAN as "Obtain an IP Address automatically" mode. This function will take effect until the router reboots.

5.5.2 DHCP Clients List

This page shows **Client Name, MAC Address, Assigned IP** and **Lease Time** for each DHCP Client attached to the router (Figure 5-13):

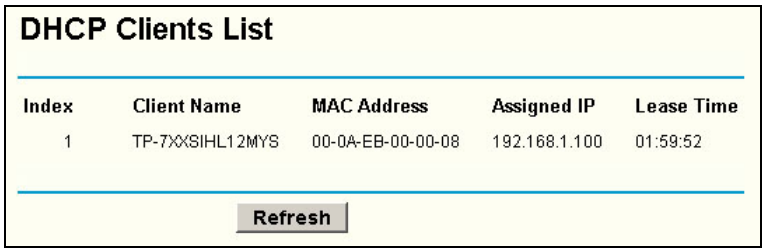


Figure 5-13 DHCP Clients List

- **Index -** The index of the DHCP Client
- **Client Name -** The name of the DHCP client
- **MAC Address -** The MAC address of the DHCP client
- **Assigned IP -** The IP address that the router has allocated to the DHCP client.
- **Lease Time -** The time of the DHCP client leased. Before the time is up, DHCP client will request to renew the lease automatically.

You cannot change any of the values on this page. To update this page and to show the current attached devices, click the **Refresh** button.

5.5.3 Address Reservation

When you specify a reserved IP address for a PC on the LAN, that PC will always receive the same IP address each time it accesses the DHCP server. Reserved IP addresses should be assigned to servers that require permanent IP settings. This page is used for address reservation (shown in Figure 5-14).

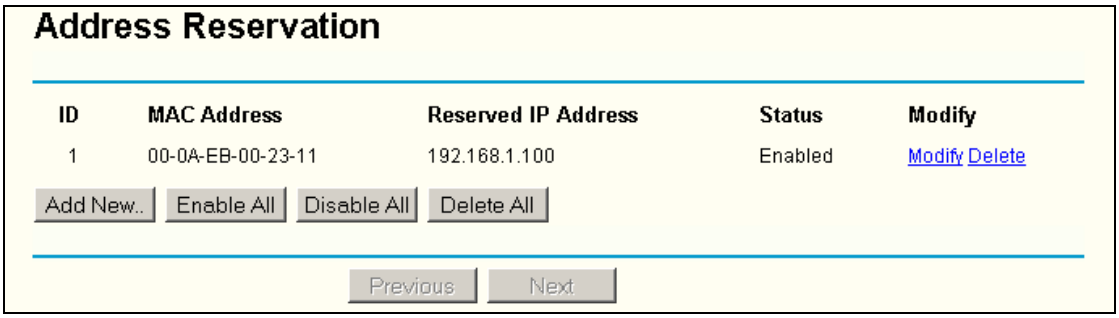


Figure 5-14 Address Reservation

- **MAC Address -** The MAC address of the PC of which you want to reserve IP address.
- **Assigned IP Address -** The IP address of the router reserved.
- **Status -** The status of this entry either **Enabled** or **Disabled**.

To Reserve IP addresses:

1. Click the **Add New button**. (Pop-up Figure 5-15)
2. Enter the MAC address (The format for the MAC Address is XX-XX-XX-XX-XX-XX.) and IP address of the computer you wish to add.
3. Click the **Save** button when finished.

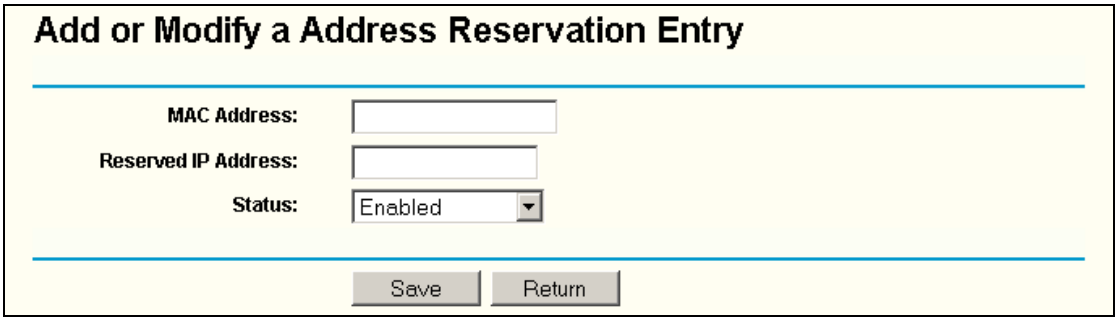


Figure 5-15 Add or Modify an Address Reservation Entry

To modify or delete an existing entry:

1. Click the **Modify** in the entry you want to modify. If you want to delete the entry, click the **Delete**.
2. Modify the information.
3. Click the **Save** button.

Click the **Enable All** button to make all entries enabled
Click the **Disabled All** button to make all entries disabled.
Click the **Delete All** button to delete all entries

Click the **Next** button to go to the next page and Click the **Previous** button to return the previous page.

Note: The function won't take effect until the router reboots.

5.6 Forwarding

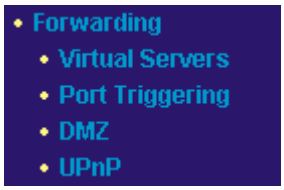


Figure 5-16 the Forwarding menu

There are four submenus under the Forwarding menu (shown in Figure 5-16): **Virtual Servers**, **Port Triggering**, **DMZ** and **UPnP**. Click any of them, and you will be able to configure the corresponding function. The detailed explanations for each submenu are provided below.

5.6.1 Virtual Servers

Virtual servers can be used for setting up public services on your LAN, such as DNS, Email and FTP. A virtual server is defined as a service port, and all requests from the Internet to this service port will be redirected to the computer specified by the server IP. Any PC that was used for a virtual server must have a static or reserved IP Address because its IP Address may change when using the DHCP function. You can set up virtual servers on this page, shown in Figure 5-17:

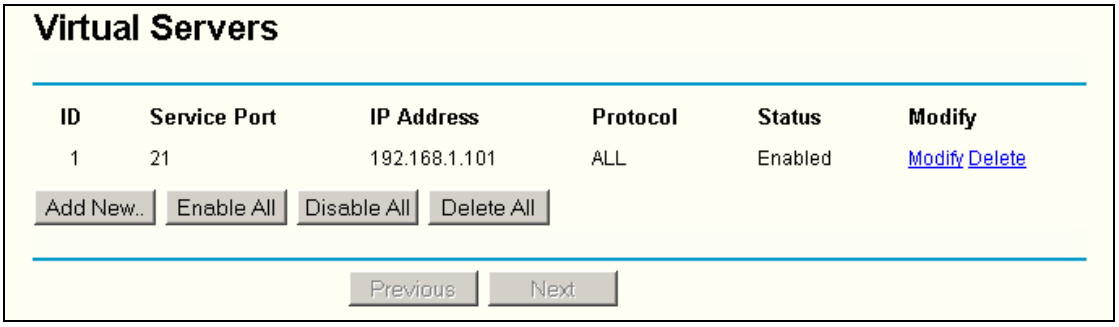


Figure 5-17 Virtual Servers

- **Service Port -** The numbers of External Ports. You can type a service port or a range of service ports (the format is XXX – YYY, XXX is the start port, YYY is the end port).
- **IP Address -** The IP Address of the PC providing the service application.
- **Protocol -** The protocol used for this application, either **TCP**, **UDP**, or **All** (all protocols supported by the router).
- **Status -** The status of this entry either **Enabled** or **Disabled**.

To setup a virtual server entry:

1. Click the **Add New button**. (pop-up Figure 5-18)
2. Select the service you want to use from the Common Service Port list. If the **Common Service Port** list does not have the service that you want to use, type the number of the service port or service port range in the **Service Port** box.
3. Type the IP Address of the computer in the **Server IP Address** box.

4. Select the protocol used for this application, either **TCP** or **UDP**, or **All**.
5. Select the **Enable** checkbox to enable the virtual server.
6. Click the **Save** button.

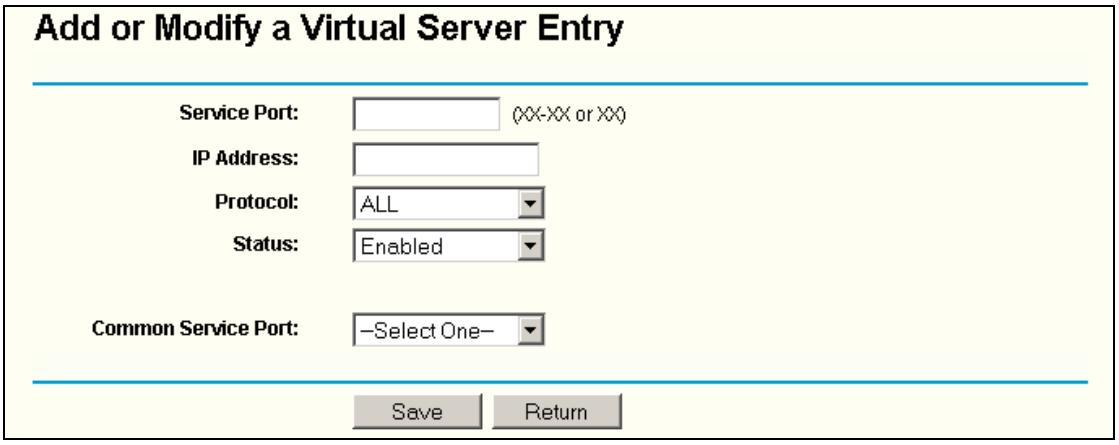


Figure 5-18 Add or Modify a Virtual Server Entry

Note: It is possible that you have a computer or server that has more than one type of available service. If so, select another service, and enter the same IP Address for that computer or server.

To modify or delete an existing entry:

1. Click the **Modify** in the entry you want to modify. If you want to delete the entry, click the **Delete**.
2. Modify the information.
3. Click the **Save** button.

Click the **Enable All** button to make all entries enabled
Click the **Disabled All** button to make all entries disabled.
Click the **Delete All** button to delete all entries

Click the **Next** button to go to the next page and Click the **Previous** button to return the previous page.

Note: If you set the virtual server of service port as 80, you must set the Web management port on **Security –> Remote Management** page to be any value except 80 such as 8080. Or else there will be a conflict to disable the virtual server.

5.6.2 Port Triggering

Some applications require multiple connections, like Internet games, video conferencing, Internet calling and so on. These applications cannot work with a pure NAT router. Port Triggering is used for some of these applications that can work with an NAT router. You can set up Port Triggering on this page shown in Figure 5-19:

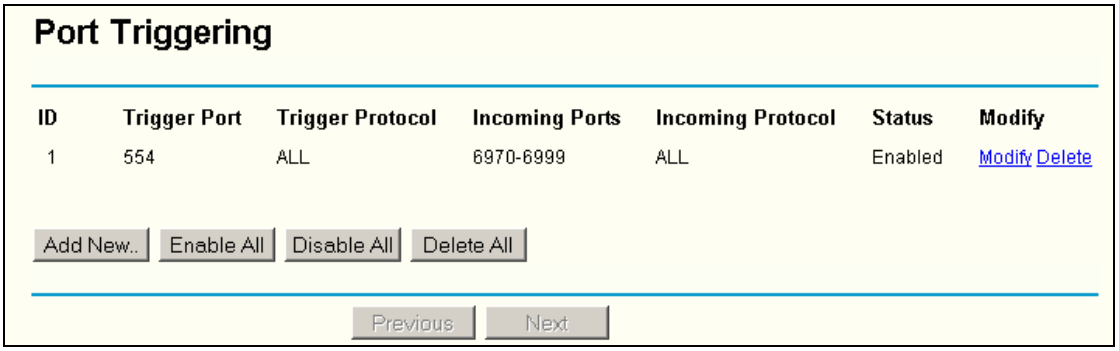


Figure 5-19 Port Triggering

Once configured, operation is as follows:

1. A local host makes an outgoing connection using a destination port number defined in the Trigger Port field.
2. The router records this connection, opens the incoming port or ports associated with this entry in the Port Triggering table, and associates them with the local host.
3. When necessary the external host will be able to connect to the local host using one of the ports defined in the **Incoming Ports** field.

- **Trigger Port -** The port for outgoing traffic. An outgoing connection using this port will "Trigger" this rule.
- **Trigger Protocol -** The protocol used for Trigger Ports, either **TCP**, **UDP**, or **All** (all protocols supported by the router).
- **Incoming Ports Range -** The port or port range used by the remote system when it responds to the outgoing request. A response using one of these ports will be forwarded to the PC that triggered this rule. You can input at most 5 groups of ports (or port section). Every group of ports must be set apart with ",". For example, 2000-2038, 2050-2051, 2085, 3010-3030.
- **Incoming Protocol -** The protocol used for Incoming Ports Range, either TCP or UDP, or ALL (all protocols supported by the router).
- **Status -** The status of this entry either **Enabled** or **Disabled**.

To add a new rule, enter the following data on the **Port Triggering** screen.

1. Click the **Add New button**. (pop-up Figure 5-20)
2. Enter a port number used by the application when it generates an outgoing request.
3. Select the protocol used for **Trigger Port** from the pull-down list, either **TCP**, **UDP**, or **All.**
4. Enter the range of port numbers used by the remote system when it responds to the PC's request.
5. Select the protocol used for **Incoming Ports Range** from the pull-down list, either **TCP** or **UDP**, or **All.**
6. Select the **Enable** checkbox to enable.
7. Click the **Save** button to save the new rule.

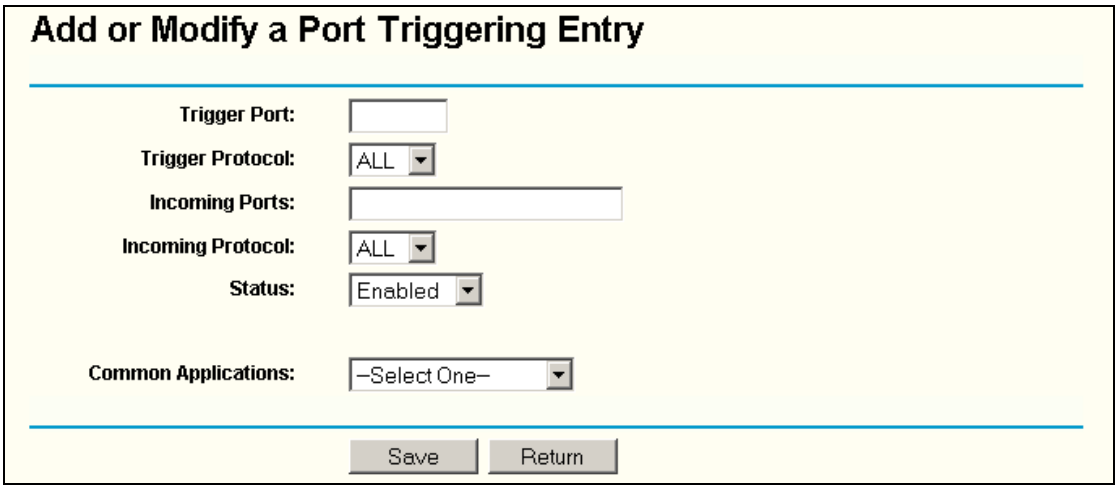


Figure 5-20 Add or Modify a Triggering Entry

There are many popular applications in the **Popular Application** list. You can select it, and the application will fill in the **Trigger Port**, **incoming Ports Range** boxes and select the **Enable** checkbox. It has the same effect as adding a new rule.

To modify or delete an existing entry:

1. Click the **Modify** in the entry you want to modify. If you want to delete the entry, click the **Delete**.
2. Modify the information.
3. Click the **Save** button.

Click the **Enable All** button to make all entries enabled
Click the **Disabled All** button to make all entries disabled.
Click the **Delete All** button to delete all entries

Note:

1. When the trigger connection is released, the according opening ports will be closed.
2. Each rule allowed to be used only by one host on LAN synchronously. The trigger connection of other hosts on LAN will be refused.
3. Incoming Port Range cannot overlap each other.

5.6.3 DMZ

The DMZ host feature allows one local host to be exposed to the Internet for a special-purpose service such as Internet gaming or videoconferencing. DMZ host forwards all the ports at the same time. Any PC whose port is being forwarded must have its DHCP client function disabled and should have a new static IP Address assigned to it because its IP Address may change when using the DHCP function. You can set up DMZ host on this page shown in Figure 5-21:

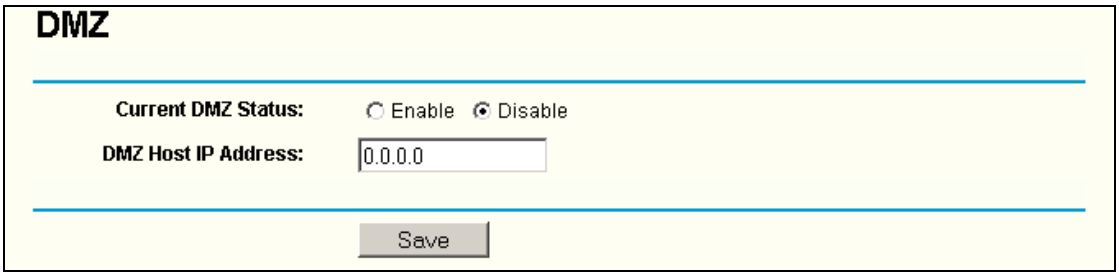


Figure 5-21 DMZ

To assign a computer or server to be a DMZ server:

1. Click the **Enable** radio button
2. Enter the local host IP Address in the **DMZ Host IP Address** field
3. Click the **Save** button.

Note: After you set the DMZ host, the firewall related to the host will not work.

5.6.4 UPnP

The Universal Plug and Play (UPnP) feature allows the devices, such as Internet computers, to access the local host resources or devices as needed. UPnP devices can be automatically discovered by the UPnP service application on the LAN. You can configure UPnP on this page that shown in Figure 5-22:

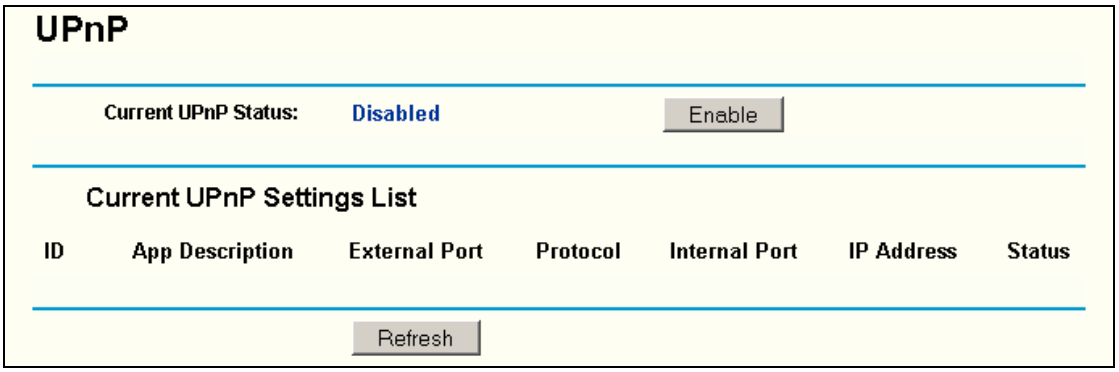


Figure 5-22 UPnP Settings

- **Current UPnP Status -** UPnP can be enabled or disabled by clicking the **Enable** or **Disable** button. As allowing this may present a risk to security, this feature is disabled by default.
- **Current UPnP Settings List -** This table displays the current UPnP information.
  - **App Description** – The description provided by the application in the UPnP request
  - **External Port -** External port, which the router opened for the application.
  - **Protocol –** Shows which type of protocol is opened.
  - **Internal Port -** Internal port, which the router opened for local host.
  - **IP Address -** The UPnP device that is currently accessing the router.
  - **Status -** Either Enabled or Disabled, “Enabled” means that port is still active. Otherwise, the port is inactive.

Click **Refresh** to update the Current UPnP Settings List.

5.7 Security

Figure 5-23 the Security menu

There are six submenus under the Security menu (shown in Figure 5-23): **Firewall**, **IP Address Filtering, Domain Filtering, MAC Filtering, Remote Management** and **Advanced Security.** Click any of them, and you will be able to configure the corresponding function. The detailed explanations for each submenu are provided below.

5.7.1 Firewall

Using the Firewall page (shown in Figure 5-24), you can turn the general firewall switch on or off. The default setting for the switch is off. If the general firewall switch is off, even if IP Address Filtering, DNS Filtering and MAC Filtering are enabled, their settings are ineffective.

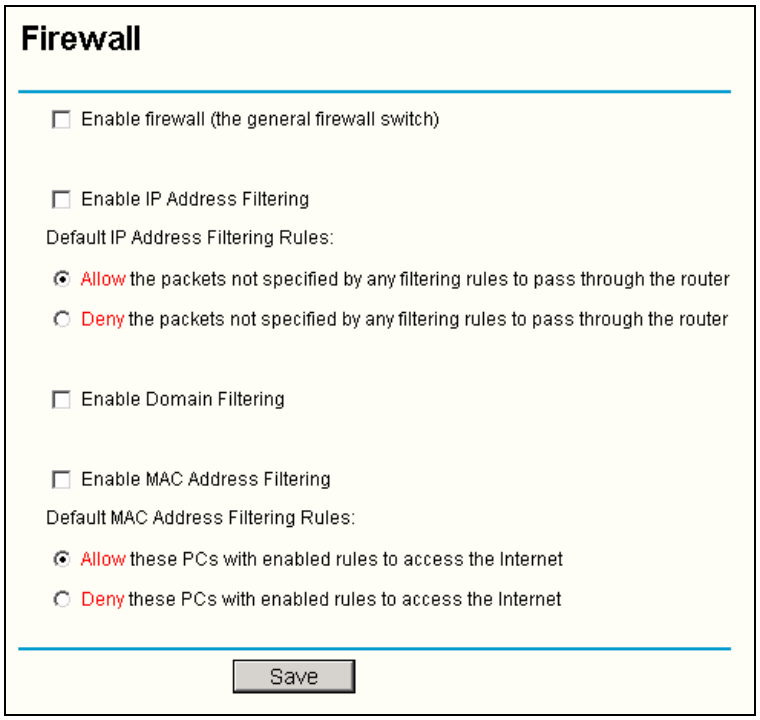

Firewall
Enable firewall (the general firewall switch)
Enable IP Address Filtering
Default IP Address Filtering Rules:
Allow the packets not specified by any filtering rules to pass through the router
Deny the packets not specified by any filtering rules to pass through the router
Enable Domain Filtering
Enable MAC Address Filtering
Default MAC Address Filtering Rules:
Allow these PCs with enabled rules to access the Internet
Deny these PCs with enabled rules to access the Internet
Save

Figure 5-24 Firewall Settings

- **Enable Firewall -** the general firewall switch is on or off.

- **Enable IP Address Filtering -** set IP Address Filtering is enabled or disabled. There are two default filtering rules of IP Address Filtering, either Allow or Reny passing through the router.
- **Enable Domain Filtering -** Set Domain Filtering as enabled or disabled.
- **Enable MAC Filtering -** Set MAC Address Filtering is enabled or disabled. You can select the default filtering rules of MAC Address Filtering, either Allow or Reny accessing the router.

5.7.2 IP Address Filtering

The IP Address Filtering feature allows you to control Internet Access by specific users on your LAN based on their IP addresses. The IP Address Filtering are set on this page, Figure 5-25:

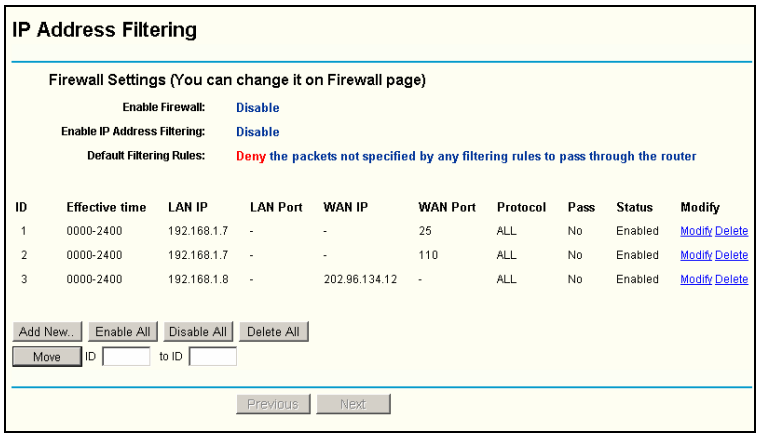

IP Address Filtering
Firewall Settings (You can change it on Firewall page)
Enable Firewall: Disable
Enable IP Address Filtering: Disable
Default Filtering Rules: Deny the packets not specified by any filtering rules to pass through the router
ID Effective time LAN IP LAN Port WAN IP WAN Port Protocol Pass Status Modify
1 0000-2400 192.168.1.7 - - 25 ALL No Enabled Modify Delete
2 0000-2400 192.168.1.7 - - 110 ALL No Enabled Modify Delete
3 0000-2400 192.168.1.8 - 202.96.134.12 - ALL No Enabled Modify Delete
Add New... Enable All Disable All Delete All
Move ID to ID
Previous Next

Figure 5-25 IP Address Filtering

To disable the IP Address Filtering feature, keep the default setting, **Disabled**. To set up an IP Address Filtering entry, click **Enable** Firewall and **Enable** IP Address Filtering on the Firewall page, and click the **Add New…** button. The page " **Add or Modify an IP Address Filtering entry** " will appear shown in Figure 5-26:

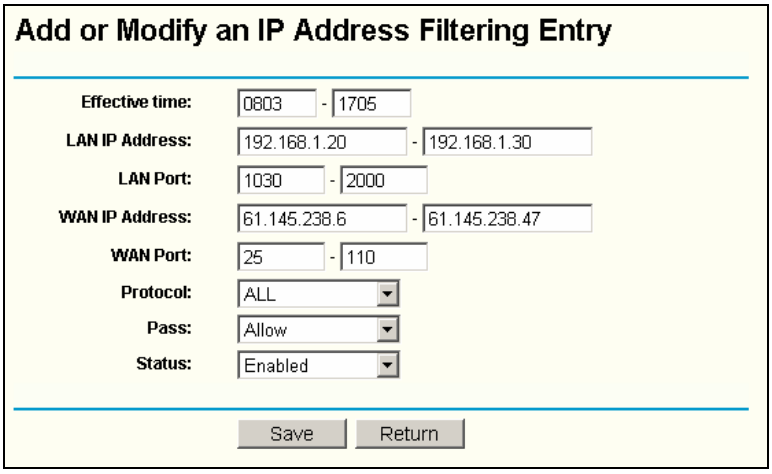

Add or Modify an IP Address Filtering Entry
Effective time: 0803 - 1705
LAN IP Address: 192.168.1.20 - 192.168.1.30
LAN Port: 1030 - 2000
WAN IP Address: 61.145.238.6 - 61.145.238.47
WAN Port: 25 - 110
Protocol: ALL
Pass: Allow
Status: Enabled
Save Return

Figure 5-26 Add or Modify an IP Address Filtering Entry

To create or modify an IP Address Filtering entry, please follow these instructions:

1. **Effective Time -** Enter a range of time in HHMM format, which point to the range time for the entry to take effect. For example, 0803 - 1705, the entry will take effect

from 08:03 to 17:05.

2. **LAN IP Address -** Type a LAN IP address or a range of LAN IP addresses in the field. For example, 192.168.1.20 - 192.168.1.30. Keep the field open, which means all LAN IP addresses have been put into the field.
3. **LAN Port -** Type a LAN Port or a range of LAN ports in the field. For example, 1030 - 2000. Keep the field open, which means all LAN ports have been put into the field.
4. **WAN IP Address -** Type a WAN IP address or a range of WAN IP addresses in the field. For example, 61.145.238.6 – 61.145.238.47. Keep the field open, which means all WAN IP addresses have been put into the field.
5. **WAN Port -** Type a WAN Port or a range of WAN Ports in the field. For example, 25 – 110. Keep the field open, which means all WAN Ports have been put into the field.
6. **Protocol -** Select which protocol is to be used, either **TCP, UDP**, or **All** (all protocols supported by the router).
7. **Pass -** Select either **Allow** or **Deny** through the router.
8. **Status -** Select **Enabled** or **Disabled** for this entry on the **Status** pull-down list.
9. Click the **Save** button to save this entry.

To add additional entries, repeat steps 1-9.
When finished, click the **Return** button to return to **IP Address Filtering** page.

To modify or delete an existing entry:

1. Find the desired entry in the table.
2. Click **Modify** or **Delete** as desired on the **Modify** column.

Click the **Enable All** button to enable all entries.
Click the **Disable All** button to disable all entries.
Click the **Delete All** button to delete all entries

You can change the entry's order as desired. Fore entries are before hind entries. Enter the ID number in the first box you want to move and another ID number in second box you want to move to, and then click the **Move** button to change the entry's order.

Click the **Next** button to go to the next page and click the **Previous** button to return to the previous page.

For example: If you desire to block E-mail received and sent by the IP address 192.168.1.7 on your local network, and wish to make the PC with IP address 192.168.1.8 unable to visit the website of IP address 202.96.134.12, while other PCs have no limit. First, enable the **Firewall** and **IP Address Filtering** on the **Firewall** page, then, you should specify the Default IP Address Filtering Rule "**Deny these PCs with effective rules to access the Internet**" on the Firewall page and the following IP address filtering list on this page:

ID	Effective time	LAN IP	LAN Port	WAN IP	WAN Port	Protocol	Pass	Status	Modify
1	0000-2400	192.168.1.7	-	-	25	ALL	No	Enabled	Modify Delete
2	0000-2400	192.168.1.7	-	-	110	ALL	No	Enabled	Modify Delete
3	0000-2400	192.168.1.8	-	202.96.134.12	-	ALL	No	Enabled	Modify Delete

5.7.3 Domain Filtering

The Domain Filtering page (shown in Figure 5-27) allows you to control access to certain websites on the Internet by specifying their domains or key words.

Figure 5-27 Domain Filtering

Before adding a Domain Filtering entry, you must ensure that **Enable** Firewall and **Enable** Domain Filtering have been selected on the Firewall page. To Add a Domain filtering entry, click the **Add New…** button. The page " **Add or Modify a Domain Filtering entry** " will appear, shown in Figure 5-28:

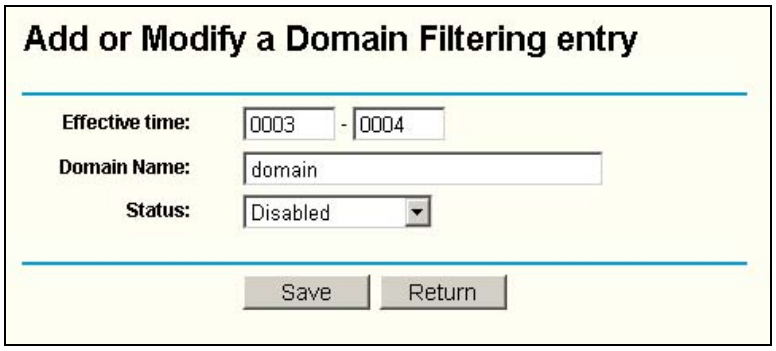


Figure 5-28 Add or Modify a Domain Filtering entry

To add or modify a Domain Filtering entry, follow these instructions:

1. **Effective Time -** Enter a range of time in HHMM format, which point to the range time for the entry to take effect. For example, 0803 - 1705, the entry will take effect from 08:03 to 17:05.
2. **Domain Name -** Type the domain or key word as desired in the field. A blank in the domain field means all websites on the Internet. For example: www.xxyy.com.cn, .net.
3. **Status -** Select **Enabled** or **Disabled** for this entry on the **Status** pull-down list.
4. Click the **Save** button to save this entry.

To add additional entries, repeat steps 1-4.

When finished, click the **Return** button to return to the **Domain filtering** page.

To Modify or delete an existing entry:

1. Find the desired entry in the table.
2. Click **Modify** or **Delete** as desired on the **Edit** column.

Click the **Enabled All** button to enable all entries.
Click the **Disable All** button disable all entries.
Click the **Delete All** button to delete all entries
Click the **Next** button to go to the next page and the **Previous** button to return to the previous page.

For example: if you want to block the PCs on your LAN from accessing websites www.xxyy.com.cn, www.aabbcc.com and websites with .net in the end on the Internet while no limit for other websites. First, enable the **Firewall** and **Domain Filtering** on the **Firewall** page, then, specify the following Domain filtering list:

ID	Effective time	Domain Name	Status	Modify
1	0000-2400	www.xxyy.com.cn	Enabled	Modify Delete
2	0800-2000	www.aabbcc.com	Enabled	Modify Delete
3	0000-2400	.net	Enabled	Modify Delete

5.7.4 MAC Filtering

Like the IP Address Filtering page, the MAC Address Filtering page (shown in Figure 5-29) allows you to control access to the Internet by users on your local network based on their MAC Addresses.

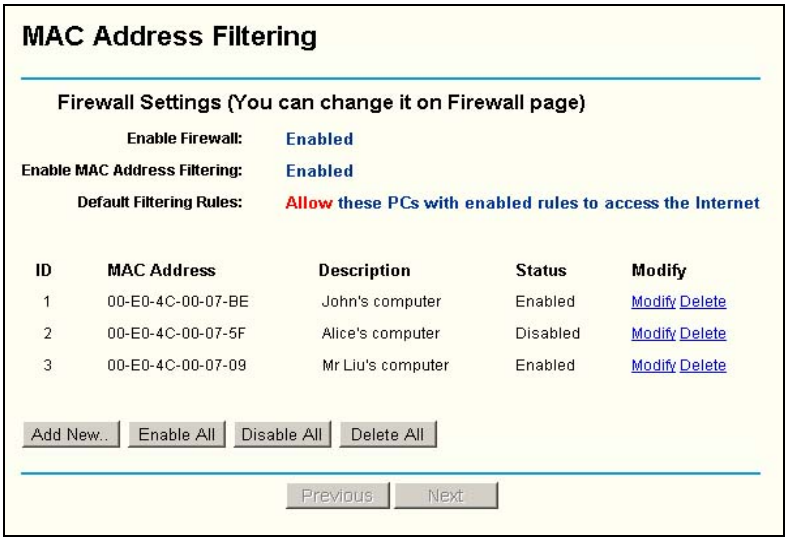

MAC Address Filtering
Firewall Settings (You can change it on Firewall page)
Enable Firewall: Enabled
Enable MAC Address Filtering: Enabled
Default Filtering Rules: Allow these PCs with enabled rules to access the Internet
ID MAC Address Description Status Modify
1 00-E0-4C-00-07-BE John's computer Enabled Modify Delete
2 00-E0-4C-00-07-5F Alice's computer Disabled Modify Delete
3 00-E0-4C-00-07-09 Mr Liu's computer Enabled Modify Delete
Add New.. Enable All Disable All Delete All
Previous Next

Figure 5-29 MAC Address Filtering

Before setting up MAC Filtering entries, you must ensure that **Enable** Firewall and **Enable** MAC Filtering have been selected on the Firewall page. To Add a MAC Address filtering entry, click the **Add New…** button. The page " **Add or Modify a MAC Address Filtering entry**" will appear, shown in Figure 5-30:

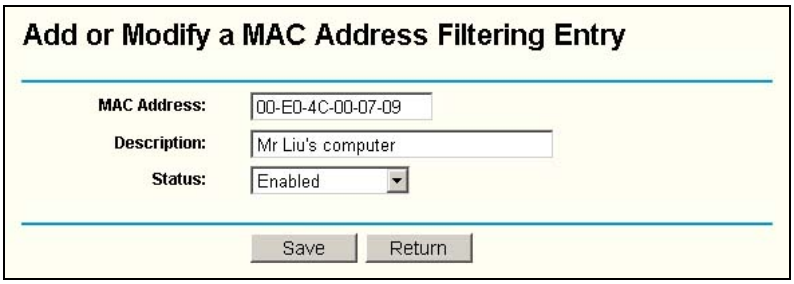


Figure 5-30 Add or Modify a MAC Address Filtering entry

To add or modify a MAC Address Filtering entry, follow these instructions:

1. Enter the appropriate MAC address into the **MAC Address** field. The format of the MAC address is XX-XX-XX-XX-XX-XX (X is any hexadecimal digit). For example: 00-0E-AE-B0-00-0B.
2. Type the description of the PC in the **Description** field. Fox example: John's PC.
3. **Status** - Select **Enabled** or **Disabled** for this entry on the **Status** pull-down list.
4. Click the **Save** button to save this entry.

To add additional entries, repeat steps 1-4.

When finished, click the **Return** button to return to the **MAC Address Filtering** page.

To Modify or delete an existing entry:

1. Find the desired entry in the table.
2. Click **Modify** or **Delete** as desired on the **Edit** column.

Click the **Enabled All** button to enable all entries.

Click the **Disable All** button disable all entries.

Click the **Delete All** button to delete all entries

Click the **Next** button to go to the next page and click the **Previous** button to return to the previous page.

Fox example: If you want to block the PCs with MAC addresses 00-0A-EB-00-07-BE and 00-0A-EB-00-07-5F to access the Internet, first, enable the **Firewall** and **MAC Address Filtering** on the **Firewall** page, then, you should specify the Default MAC Address Filtering Rule "**Deny these PCs with effective rules to access the Internet**" on the Firewall page and the following MAC address filtering list on this page:

ID	MAC Address	Description	Status	Modify
1	00-0A-EB-00-07-BE	John's computer	Enabled	Modify Delete
2	00-0A-EB-00-07-5F	Alice's Computer	Enabled	Modify Delete

5.7.5 Remote Management

You can configure the Remote Management function on this page shown in Figure 5-31. This feature allows you to manage your Router from a remote location, via the Internet.

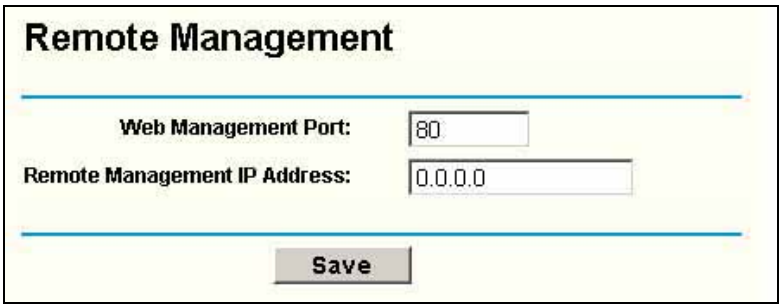


Figure 5-31 Remote Management

- **Web Management Port -** Web browser access normally uses the standard HTTP service port 80. This router's default remote management web port number is 80. For greater security, you can change the remote management web interface to a custom port by entering that number in the box provided. Choose a number between 1024 and 65534, but do not use the number of any common service port.
- **Remote Management IP Address -** This is the current address you will use when accessing your router from the Internet. The default IP address is 0.0.0.0. It means this function is disabled. To enable this function, change the default IP Address to another IP Address as desired.

To access the router, you will type your router's WAN IP address into your browser's address (in IE) or Location (in Navigator) box, followed by a colon and the custom port number. For example, if your Router's WAN address is 202.96.12.8 and you use port number 8080, enter in your browser: http://202.96.12.8:8080. You will be asked for the router's password. After successfully entering the password, you will be able to access the router's web-based utility.

Note: Be sure to change the router's default password to a very secure password.

5.7.6 Advanced Security

Using Advanced Security page (shown in Figure 5-32), you can protect the router from being attacked by TCP-SYN Flood, UDP Flood and ICMP-Flood from LAN.

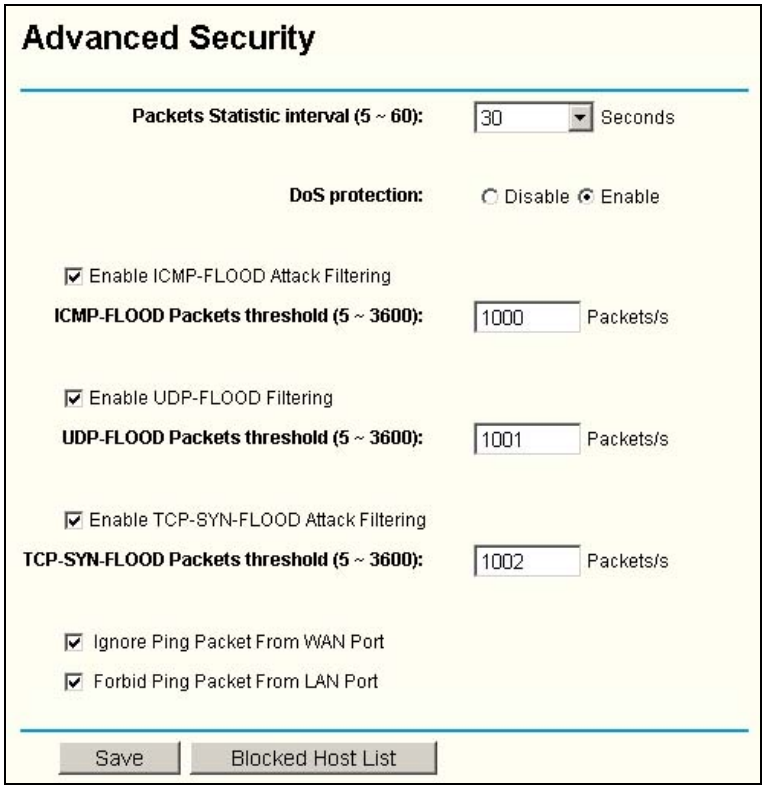


Figure 5-32 Advanced Security settings

- **Packets Statistic interval (5 ~ 60) -** The default value is 10. Select a value between 5 and 60 seconds in the pull-down list. The **Packets Statistic interval** value indicates the time section of the packets statistic. The result of the statistic used for analysis by **SYN Flood**, **UDP Flood** and **ICMP-Flood**.
- **DoS protection - Enable** or **Disable** the DoS protection function. Only when it is enabled, will the flood filters be effective.
- **Enable ICMP-FLOOD Attack Filtering - Enable** or **Disable** the **ICMP-FLOOD** Attack Filtering.
- **ICMP-FLOOD Packets threshold: (5 ~ 3600) -** The default value is 50. Enter a value between 5 ~ 3600 packets. When the current **ICMP-FLOOD** Packets numbers are beyond the set value, the router will start up the blocking function immediately.
- **Enable UDP-FLOOD Filtering - Enable** or **Disable** the **UDP-FLOOD** Filtering.
- **UDP-FLOOD Packets threshold: (5 ~ 3600) -** The default value is 50. Enter a value between 5 ~ 3600 packets. When the current **UPD-FLOOD** Packets numbers are beyond the set value, the router will start up the blocking function immediately.
- **Enable TCP-SYN-FLOOD Attack Filtering - Enable** or **Disable** the **TCP-SYN-FLOOD** Attack Filtering.
- **TCP-SYN-FLOOD Packets threshold: (5 ~ 3600) -** The default value is 50. Enter a value between 5 ~ 3600 packets. When the current **TCP-SYN-FLOOD** Packets numbers is beyond the set value, the router will start up the blocking function immediately.
- **Ignore Ping Packet from WAN Port - Enable** or **Disable** ignore ping packet from

WAN port. The default is disabled. If enabled, the ping packet from the Internet cannot access the router.

- **Forbid Ping Packet from LAN Port -** Enable or Disable forbidding Ping Packet to access the router from the LAN port. The default value is disabled. If enabled, the ping packet from the LAN port cannot access the router. (Defends against some viruses)

Click the **Save** button to save the settings.

Click the **Blocked DoS Host Table** button to display the DoS host table by blocking. The page will appear that shown in Figure 5-33:

Figure 5-33 Thwarted DoS Host Table

This page shows **Host IP Address** and **Host MAC Address** for each host blocked by the router.

- **Host IP Address** - The IP addresses that are blocked by DoS are displayed here.
- **Host MAC Address** - The MAC addresses that are blocked by DoS are displayed here.

To update this page and to show the current blocked host, click on the **Refresh** button.
Click the **Clear All** button to clear all displayed entries. After the table is empty the blocked host will regain the capability to access the Internet.
Click the **Return** button to return to the **Advanced Security** page

5.8 Static Routing

A static route is a pre-determined path that network information must travel to reach a specific host or network. To add or delete a route, work in the area under the Static Routing page (shown in Figure 5-34).

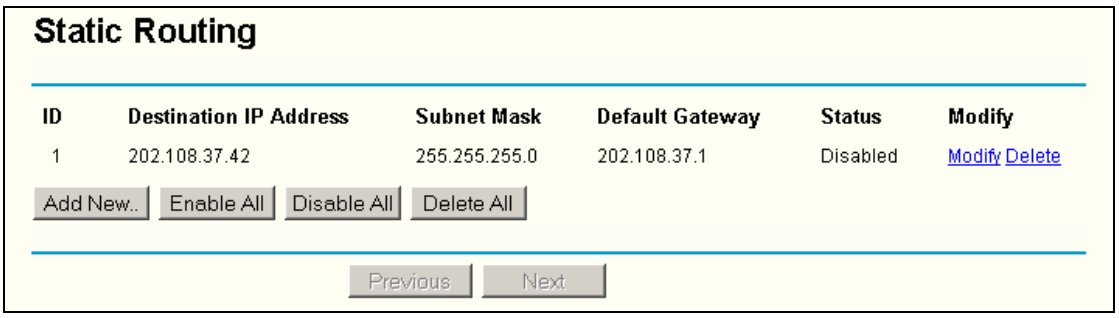


Figure 5-34 Static Routing

To add static routing entries:

1. Click the **Add New** button. (pop-up Figure 5-35)
2. Enter the following data:

- **Destination IP Address -** The **Destination IP Address** is the address of the network or host that you want to assign to a static route.
- **Subnet Mask -** The **Subnet Mask** determines which portion of an IP Address is the network portion, and which portion is the host portion.
- **Gateway -** This is the IP Address of the gateway device that allows for contact between the router and the network or host.

3. Select **Enabled** or **Disabled** for this entry on the **Status** pull-down list.
4. Click the **Save** button to save it.

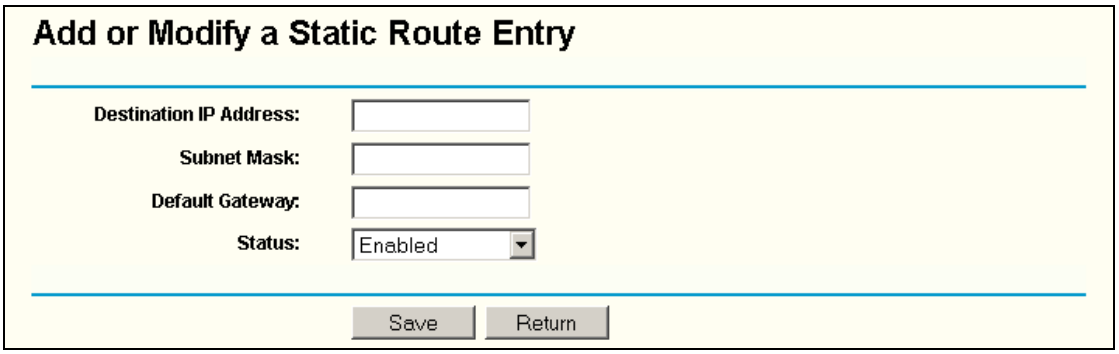


Figure 5-35 Add or Modify a Static Route Entry

To modify or delete an existing entry:

1. Click the **Modify** in the entry you want to modify. If you want to delete the entry, click the **Delete**.
2. Modify the information.
3. Click the **Save** button.

Click the **Enable All** button to make all entries enabled.
Click the **Disabled All** button to make all entries disabled.
Click the **Delete All** button to delete all entries

5.9 IP & MAC Binding Setting

Figure 5-36 the IP & MAC Binding menu

There are two submenus under the IP &MAC Binding menu (shown in Figure 5-36): **Binding Setting** and **ARP List**. Click any of them, and you will be able to scan or configure the corresponding function. The detailed explanations for each submenu are provided below.

5.9.1 Binding Setting

This page displays the IP & MAC Binding Setting table, you can operate it in accord with your desire. (shown in Figure 5-37).

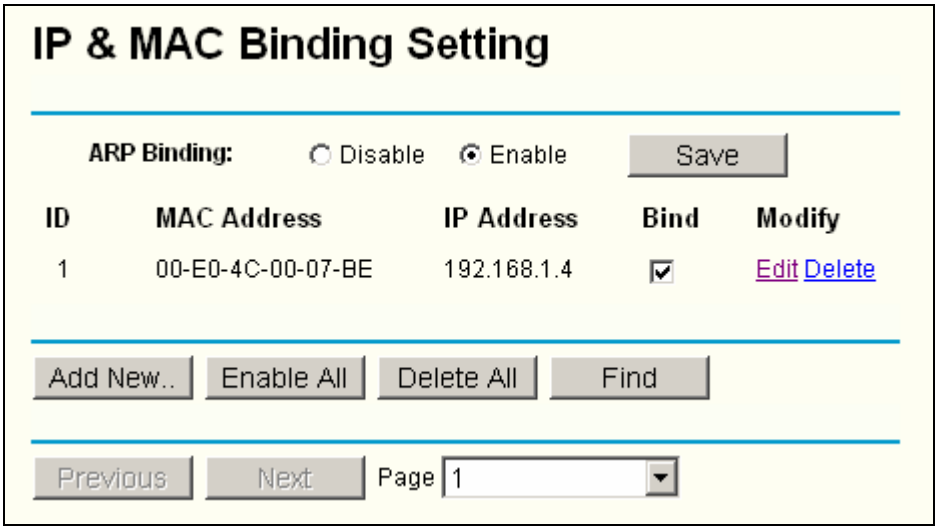


Figure 5-37 IP & MAC Binding Setting

- **MAC Address -** The MAC address of the controlled computer(s) in the LAN.
- **IP Address -** The assigned IP address of the controlled computer(s) in the LAN.
- **Bind –** Enable or disable the arp binding.
- **Modify -** Edit or delete item.

When you want to add or modify an IP & MAC Binding entry, you can click the **Add New** button or **Modify** button, then you will go to the next page. This page is used for adding or modifying an IP & MAC Binding entry (shown in Figure 5-38).

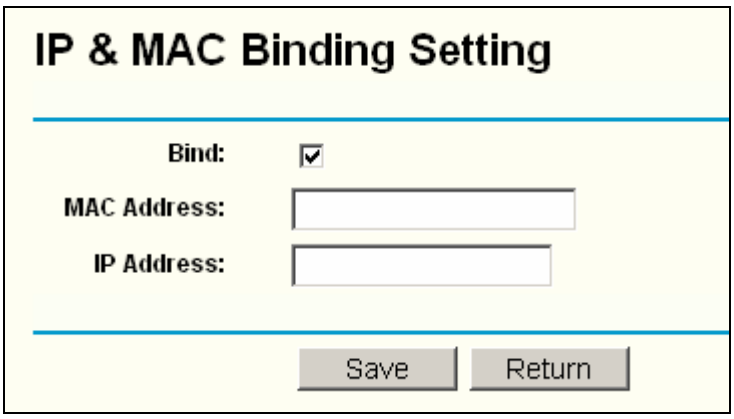


Figure 5-38 IP & MAC Binding Setting (Add & Modify)

To add IP & MAC Binding entries:

1. Click the **Add New..** button.
2. Enter the MAC Address and IP Address.
3. Select the Bind checkbox.
4. Click the **Save** button to save it.

To modify or delete an existing entry:

1. Find the desired entry in the table.
2. Click **Modify** or **Delete** as desired on the **Modify** column.

To find an existing entry:

1. Click the **Find** button (shown in Figure 5-37).
2. Enter the MAC Address or IP Address.
3. Click the **Find** button in the next page (shown in Figure 5-39).

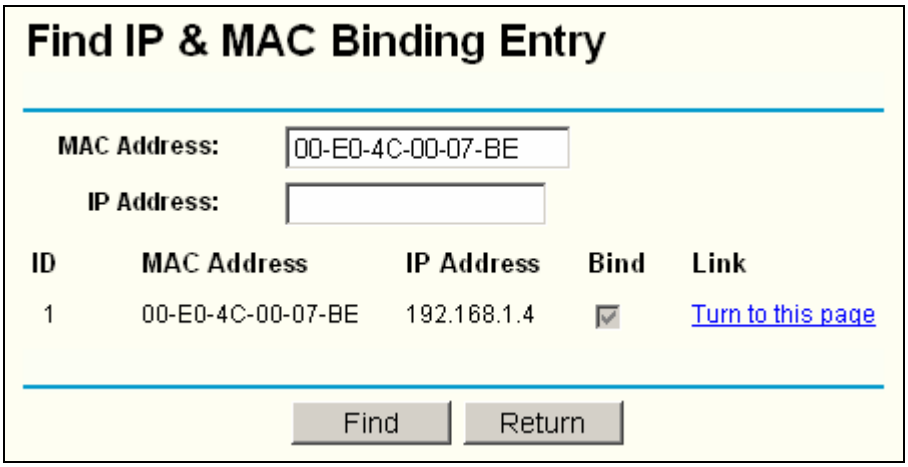


Figure 5-39 Find IP & MAC Binding Entry

Click the **Enable All** button to make all entries enabled.

Click the **Delete All** button to delete all entries.

5.9.2 ARP List

To manage the computer, you could observe the computers in the LAN by checking the relationship of MAC address and IP address in the ARP list, and you can also configure the items in the ARP list. This page displays the ARP List, it shows all the existing IP &

MAC Binding entries (shown in Figure 5-40).

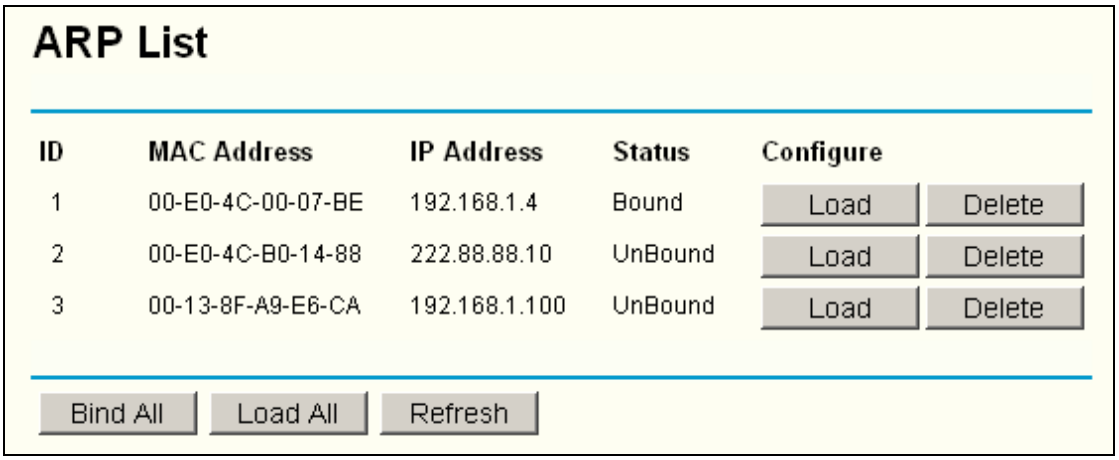


Figure 5-40 ARP List

- **MAC Address** - The MAC address of the controlled computer in the LAN.
- **IP Address** - The assigned IP address of the controlled computer in the LAN.
- **Status** - To show the MAC address and IP address binding is enabled or not.
- **Configure** - Load or delete item.
- **Load** - Load the item to the IP & MAC Binding list.
- **Delete** - Delete the item.

Click the **Bind All** button to bind all the current items, available after enable.

Click the **Load All** button to load all items to the IP & MAC Binding list.

Click the **Refresh** button to refresh all items.

Note: An item could not be loaded to the IP & MAC Binding list if the IP address of the item has been loaded before. Error warning will prompt as well. Likewise, "Load All" only loads the items without interference to the IP & MAC Binding list.

5.10 DDNS

The router offers a Dynamic Domain Name System (**DDNS**) feature. DDNS allows you to assign a fixed host and domain name to a dynamic Internet IP Address. It is useful when you are hosting your own website, FTP server, or other server behind the router. Before using this feature, you need to sign up for DDNS service providers such as www.dyndns.org, www.oray.net or www.comexe.cn. The Dynamic DNS client service provider will give you a password or key.
To set up for DDNS, follow these instructions

5.10.1 Dyndns.org DDNS

If your selected dynamic DNS **Service Provider** is www.dyndns.org, the page will

appear as shown in Figure 5-41:

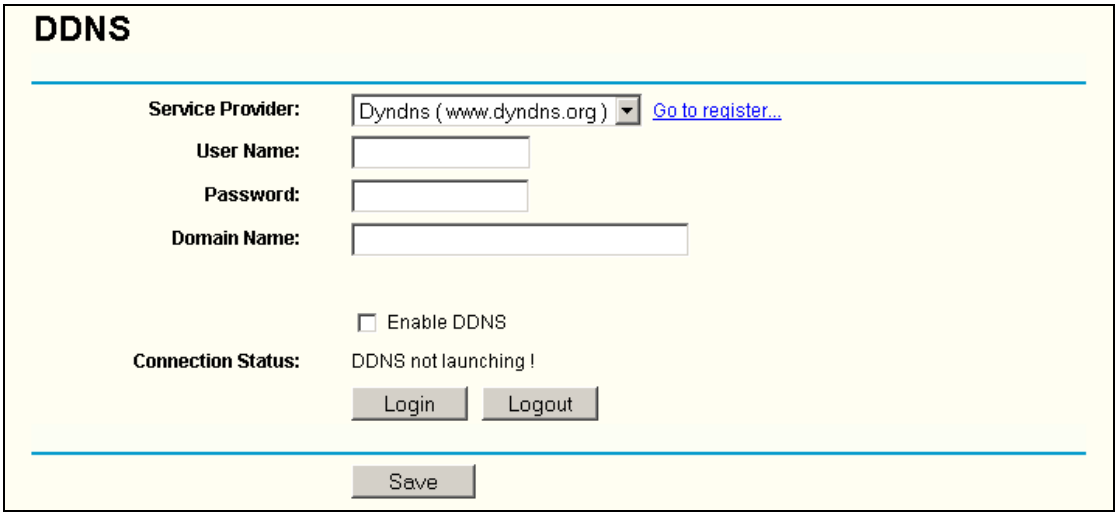


Figure 5-41 Dyndns.org DDNS Settings

To set up for DDNS, follow these instructions:

1. Type the **domain name** your dynamic DNS service provider gave.
2. Type the **User Name** for your DDNS account.
3. Type the **Password** for your DDNS account.
4. Click the **Login** button to login to the DDNS service.

- **Connection Status -**The status of the DDNS service connection is displayed here.

Click **Logout** to logout of the DDNS service.

5.10.2 Oray.net DDNS

If your selected dynamic DNS **Service Provider** is www.oray.net, the page will appear as shown in Figure 5-42:

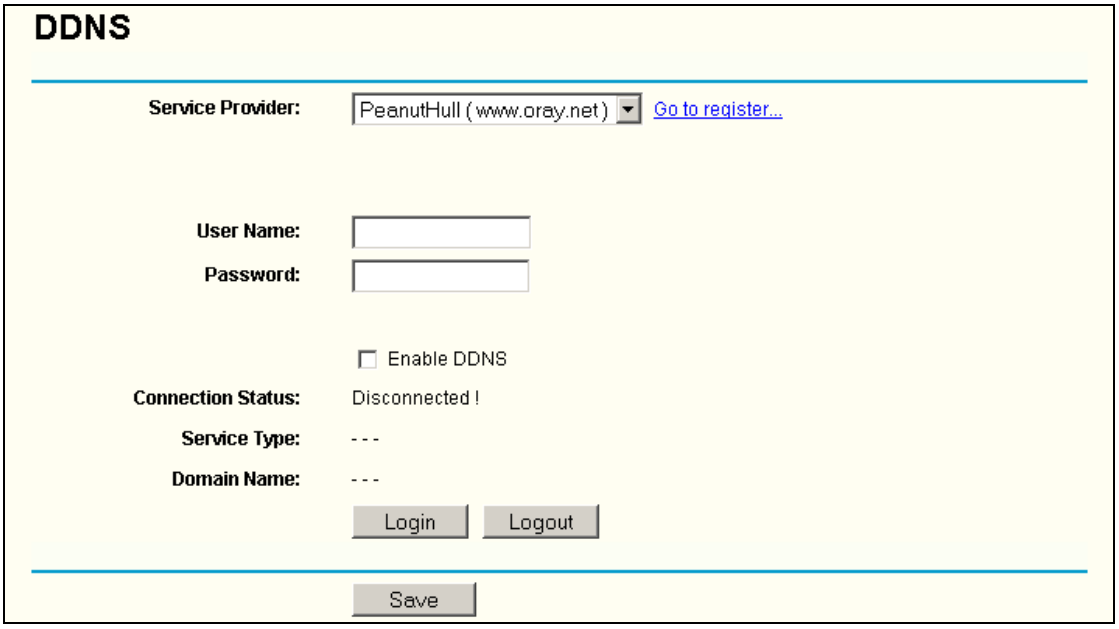


Figure 5-42 Oray.net DDNS Settings

To set up for DDNS, follow these instructions:

1. Type the **User Name** for your DDNS account.
2. Type the **Password** for your DDNS account.
3. Click the **Login** button to login the DDNS service.

- **Connection Status -** The status of the DDNS service connection is displayed here.
- **Domain Name -** The domain names are displayed here.

Click **Logout** to logout the DDNS service.

5.10.3 Comexe.cn DDNS

If your selected dynamic DNS **Service Provider** is www.comexe.cn, the page will appear as shown in Figure 5-43:

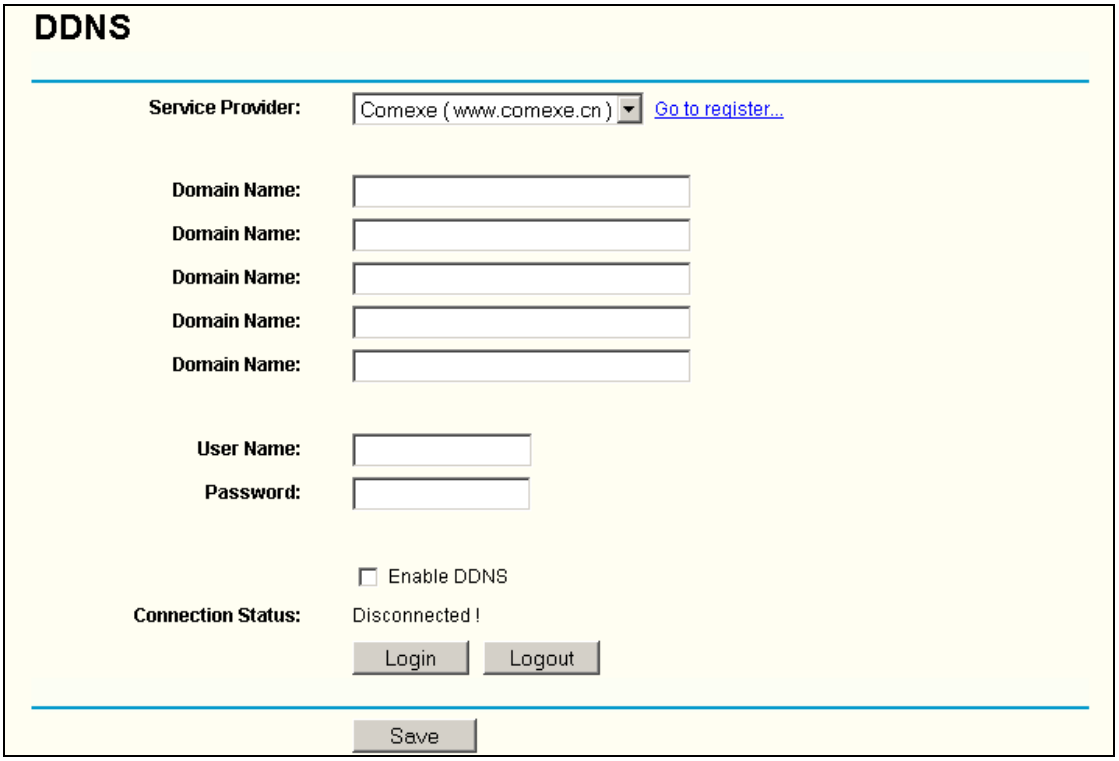


Figure 5-43 Comexe.cn DDNS Settings

To set up for DDNS, follow these instructions:

1. Type the **domain names** your dynamic DNS service provider gave.
2. Type the **User Name** for your DDNS account.
3. Type the **Password** for your DDNS account.
4. Click the **Login** button to login to the DDNS service.

- **Connection Status -**The status of the DDNS service connection is displayed here.

Click **Logout** to logout of the DDNS service.

5.11 System Tools

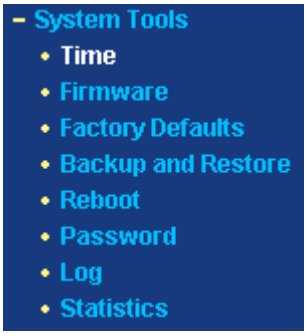


Figure 5-44 the System Tools menu

There are seven submenus under the System Tools menu (shown in Figure 5-44): **Time**, **Firmware**, **Factory Defaults, Backup and Restore, Reboot, Password, Log** and **Statistics.** Click any of them, and you will be able to configure the corresponding function. The detailed explanations for each submenu are provided below.

5.11.1 Time

You can set the time manually or get GMT from the Internet for the router on this page (shown in Figure 5-45):

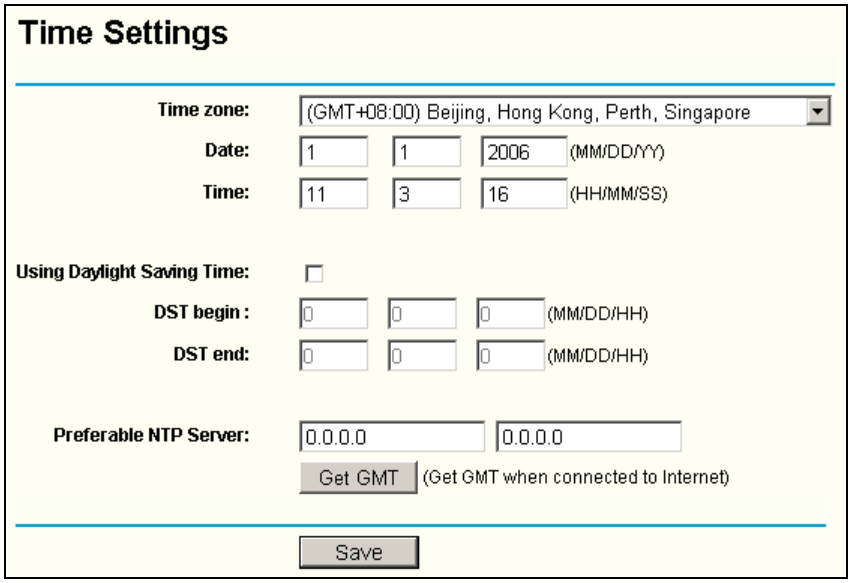


Figure 5-45 Time settings

- **Time Zone** - Select your local time zone from this pull down list.
- **Date** - Enter your local date in MM/DD/YY into the right blanks.
- **Time** - Enter your local time in HH/MM/SS into the right blanks.

Time setting follows these steps below:

1. Select your local time zone.
2. Enter date and time in the right blanks
3. Click **Save**.

Click the **Get GMT** button to get GMT time from Internet if you have connected to the

Internet.

Note:

1. This setting will be used for some time-based functions such as firewall. You must specify your time zone once you login to the router successfully, if not the time limited on these functions will not take effect.
2. The time will be lost if the router is turned off.
3. The router will obtain GMT automatically from Internet if it has already connected to Internet.

5.11.2 Firmware

The page (shown in Figure 5-46) allows you to upgrade to the latest version of firmware for the router.

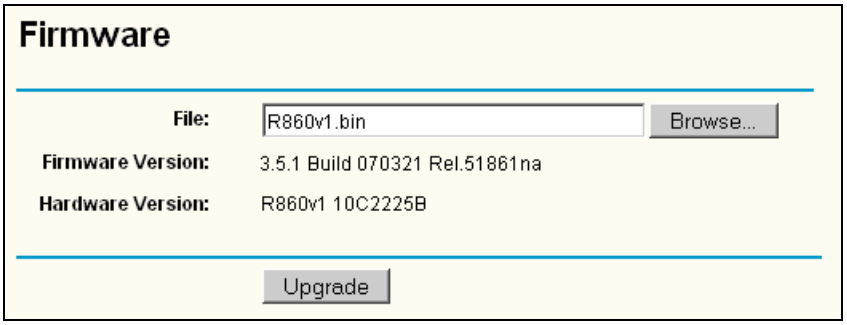


Figure 5-46 Firmware Upgrade

New firmware versions are posted at www.tp-link.com and can be downloaded for free. If the router is not experiencing difficulties, there is no need to download a more recent firmware version, unless the version has a new feature that you want to use.

Note: When you upgrade the router's firmware, you may lose its configuration settings, so make sure you write down the router settings before you upgrade its firmware.

To upgrade the router's firmware, follow these instructions:

1. Download the latest firmware upgrade file from the TP-LINK website (www.tp-link.com).
2. Run a TFTP Server on a PC on your LAN, and take the file in the TFTP server's path.
3. Type the downloaded file name into the **File Name** box.
4. Type the IP address of the PC that runs the TFTP server in the **TFTP Server's IP Address** field.
5. Click the **Upgrade** button.

- **Firmware Version -** displays the current firmware version.
- **Hardware Version -** displays the current hardware version. The hardware version of the upgrade file must accord with the current hardware version.

Note:

1. **Do not turn off the router or press the Reset button while the firmware is being upgraded.**

2. The router will reboot after the upgrade has finished.

5.11.3 Factory Defaults

This page (shown in Figure 5-47) allows you to restore the factory default settings for the router.

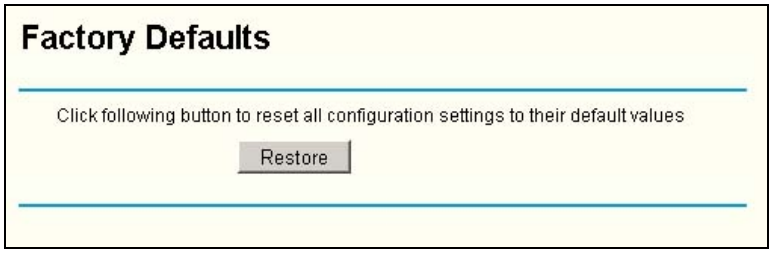


Figure 5-47 Restore Factory Default

Click the **Restore** button to reset all configuration settings to their default values.

- The default **User Name**: admin
- The default **Password**: admin
- The default **IP Address**: 192.168.1.1
- The default **Subnet Mask**: 255.255.255.0

Note: Any settings you have saved will be lost when the default settings are restored.

5.11.4 Backup and Restore

This page (shown in Figure 5-48) allows you to save current configuration of the router to a special file backup or restore the configuration file you saved before.

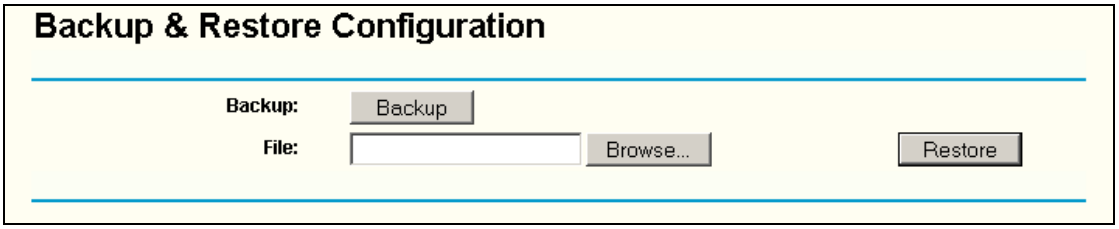


Figure 5-48 Backup & Restore Configuration

- Click the **Backup** button to save all configuration settings as a backup file in your local computer.
- To restore the router's configuration, follow these instructions:
  - Click the **Browse** button to select the backup file which you want to restore.
  - Click the **Restore** button.

Note: The current configuration will be covered with the uploaded configuration file. The restoration process will last for about 20 seconds and the router will restart automatically. Keep the router on during the restoring process, to prevent any damage.

5.11.5 Reboot

This page (shown in Figure 5-49) allows you to reboot the router.

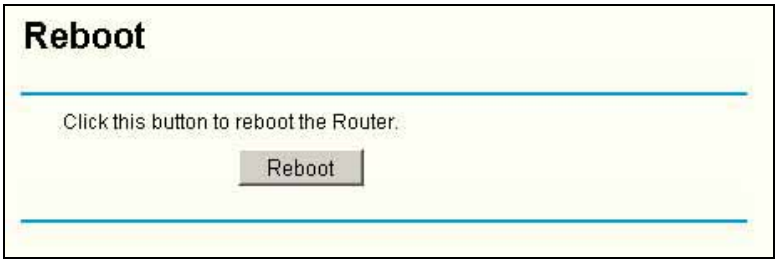


Figure 5-49 Reboot the router

Click the **Reboot** button to reboot the router.

Some settings of the router will take effect only after rebooting, which include:

- Change LAN IP Address. (System will reboot automatically)
- MAC Clone (system will reboot automatically)
- DHCP service function.
- Static address assignment of DHCP server.
- Web Service Port of the router.
- Upgrade the firmware of the router (system will reboot automatically).
- Restore the router's settings to factory default (system will reboot automatically).

5.11.6 Password

This page (shown in Figure 5-50) allows you to change the user name and password of the router.

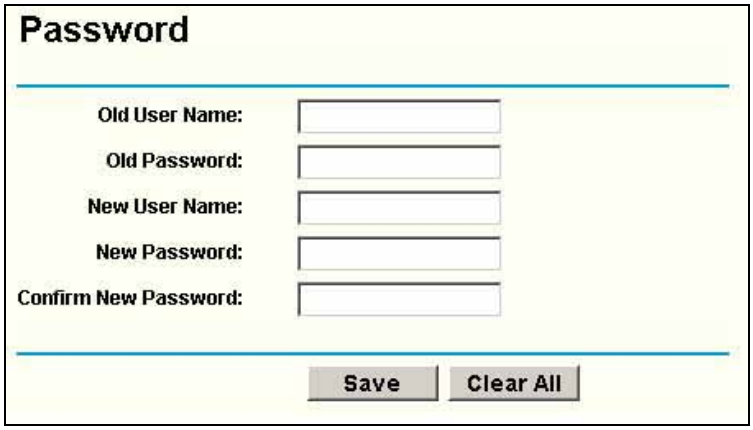


Figure 5-50 Password

It is strongly recommended that you change the factory default user name and password of the router. All users who try to access the router's web-based utility will be prompted for the router's user name and password.

Note: The new user name and password must not exceed 14 characters in length and must not include any spaces. Enter the new Password twice to confirm it.

Click the **Save** button when finished.

Click the **Clear All** button to clear all.

5.11.7 Log

This page (shown in Figure 5-51) allows you to query the Logs of the router.

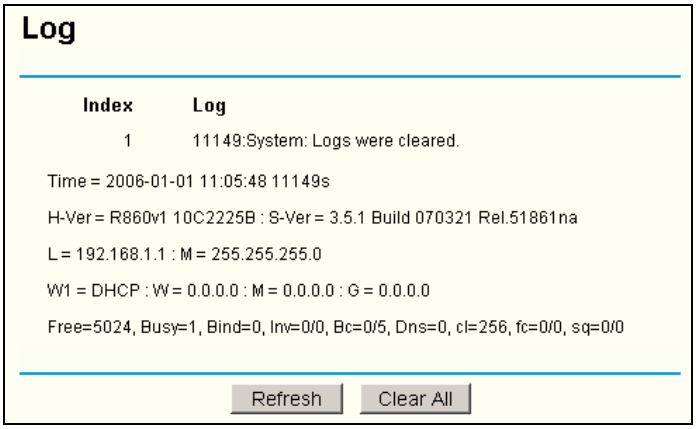

Log
Index
Log
1
11149:System: Logs were cleared.
Time = 2006-01-01 11:05:48 11149s
H-Ver = R860v1 10C2225B : S-Ver = 3.5.1 Build 070321 Rel.51861na
L = 192.168.1.1 : M = 255.255.255.0
W1 = DHCP : W = 0.0.0.0 : M = 0.0.0.0 : G = 0.0.0.0
Free=5024, Busy=1, Bind=0, Inv=0/0, Bc=0/5, Dns=0, cl=256, fc=0/0, sq=0/0
Refresh
Clear All

Figure 5-51 System Log

The router can keep logs of all traffic. You can query the logs to find what happened to the router.

Click the **Refresh** button to refresh the logs.

Click the **Clear Log** button to clear all the logs.

5.11.8 Statistics

The Statistics page (shown in Figure 5-52) displays the network traffic of each PC on LAN, including total traffic and traffic of the last **Packets Statistic interval** seconds.

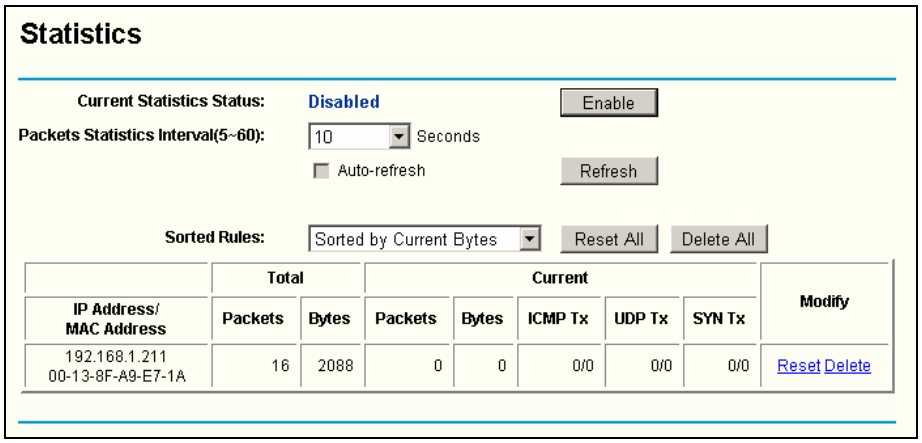


Figure 5-52 Statistics

- **Current Statistics Status -** Enable or Disable. The default value is disabled. To enable, click the **Enable** button. If disabled, the function of DoS protection in Security settings will be ineffective.
- **Packets Statistics Interval -** The default value is 10. Select a value between 5 and 60 seconds in the pull-down list. The Packets Statistic interval value indicates the time section of the packets statistic.
- **Sorted Rules -** This displays sort as desired.

Statistics Table:

IP Address		The IP address displayed with statistics
Total	**Packets**	The total amount of packets received and transmitted by the router.
	Bytes	The total amount of bytes received and transmitted by the router.
Current	**Packets**	The total amount of packets received and transmitted in the last **Packets Statistic interval** seconds.
	Bytes	The total amount of bytes received and transmitted in the last **Packets Statistic interval** seconds.
	ICMP Tx	The total amount of the ICMP packets transmitted to WAN in the last **Packets Statistic interval** seconds.
	UDP Tx	The total amount of the UDP packets transmitted to WAN in the last **Packets Statistic interval** seconds.
	TCP SYN Tx	The total amount of the TCP SYN packets transmitted to WAN in the last **Packets Statistic interval** seconds.

Click the **Save** button to save the **Packets Statistic interval** value.

Click the **Auto-refresh** checkbox to refresh automatically.

Click the **Refresh** button to refresh immediately.

Appendix A: FAQ

1. How do I configure the router to access Internet by ADSL users?

1) First, configure the ADSL modem configured in RFC1483 bridge model.
2) Connect the Ethernet cable from your ADSL modem to the WAN port on the router. The telephone cord plugs into the Line port of the ADSL modem.
3) Login to the router, click the “Network” menu on the left of your browser, and click "WAN" submenu. On the WAN page, select “PPPoE” for WAN Connection Type. Type user name in the “User Name” field and password in the “Password” field, finish by clicking “Connect”.

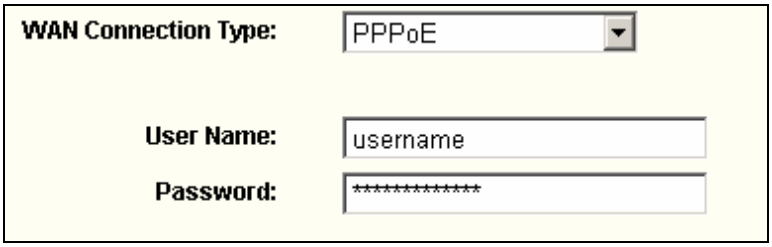


Figure A-1 PPPoE Connection Type

4) If your ADSL lease is in “pay-according-time” mode, select “Connect on Demand” or “connect Manually” for Internet connection mode. Type an appropriate number for “Max Idle Time” to avoid wasting paid time. Otherwise, you can select “Auto-connecting” for Internet connection mode.

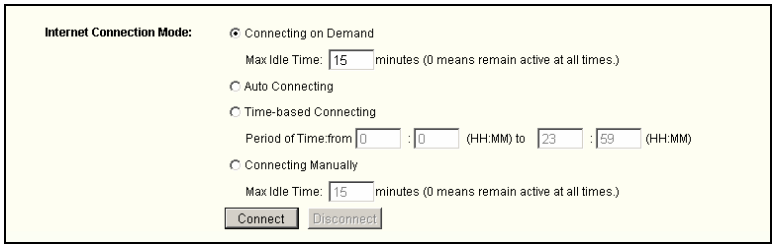

Internet Connection Mode:
Connecting on Demand
Max Idle Time: 15 minutes (0 means remain active at all times.)
Auto Connecting
Time-based Connecting
Period of Time:from 0 : 0 (HH:MM) to 23 : 59 (HH:MM)
Connecting Manually
Max Idle Time: 15 minutes (0 means remain active at all times.)
Connect
Disconnect

Figure A-2 PPPoE Connection Mode

Note:

i. Sometimes the connection cannot be disconnected although you specify a time to Max Idle Time, since some applications visit the Internet continually in the background.

ii. If you are a Cable user, please configure the router following the above steps.

2. How do I configure the router to access Internet by Ethernet users?

1) Login to the router, click the “Network” menu on the left of your browser, and click "WAN" submenu. On the WAN page, select “Dynamic IP” for "WAN Connection Type", finish by clicking “Save”.
2) Some ISPs require that you register the MAC address of your adapter, which is connected to your cable or DSL modem during installation. If your ISP requires

MAC register, login to the router and click the "Network" menu link on the left of your browser, and then click "MAC Clone" submenu link. On the "MAC Clone" page, if your PC's MAC address is a proper MAC address, click the "Clone MAC Address" button and your PC's MAC address will fill in the "WAN MAC Address" field. Or else, type the MAC address into the " WAN MAC Address" field. The format for the MAC address is XX-XX-XX-XX-XX-XX. Then click the "Save" button. It will take effect after rebooting.

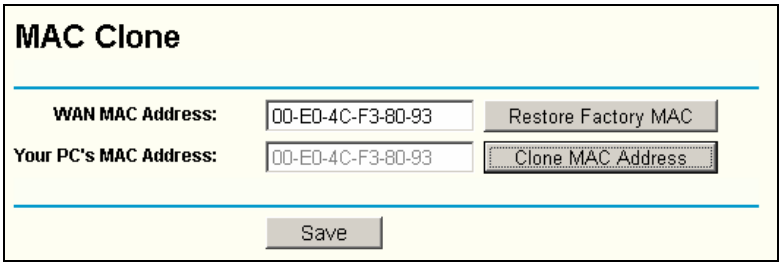


Figure A-3 MAC Clone

3. I want to use Netmeeting, what do I need to do?

1) If you start Netmeeting as a sponsor, you don't need to do anything with the router.
2) If you start as a responsor, you need configure Virtual Server or DMZ Host.
3) How to configure Virtual Server: Login to the router, click the "Forwarding" menu on the left of your browser, and click " Virtual Servers" submenu. On the "Virtual Server" page, enter "1720" into the blank below the "Service Port", and your IP address below the IP Address, assuming 192.168.1.169 for an example, remember to "Enable" and "Save".

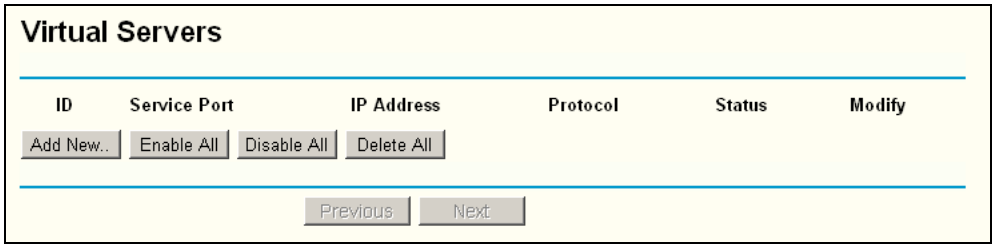
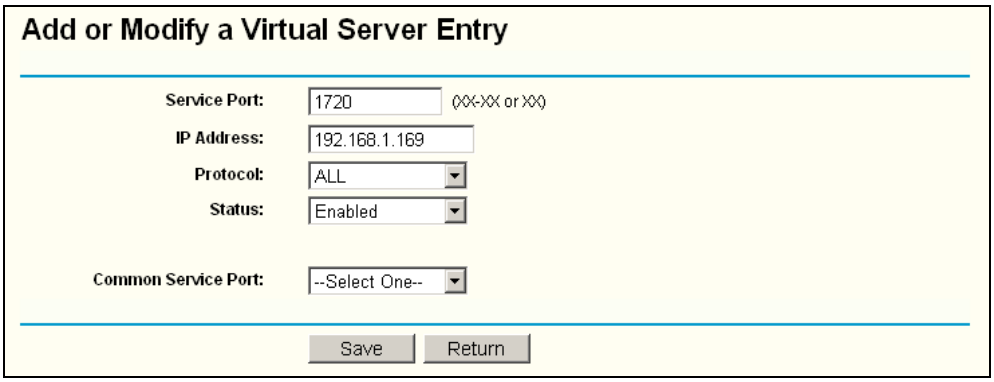


Figure A-4 Virtual Server



A-5 Add or Modify a Virtual server Entry

Note: Your opposite side should call your WAN IP, which is displayed on the

"Status" page.

4) How to enable DMZ Host: Login to the router, click the "Forwarding" menu on the left of your browser, and click " DMZ" submenu. On the "DMZ" page, click "Enable" radio and type your IP address into the "DMZ Host IP Address" field, using 192.168.1.169 as an example, remember to click the "Save" button.

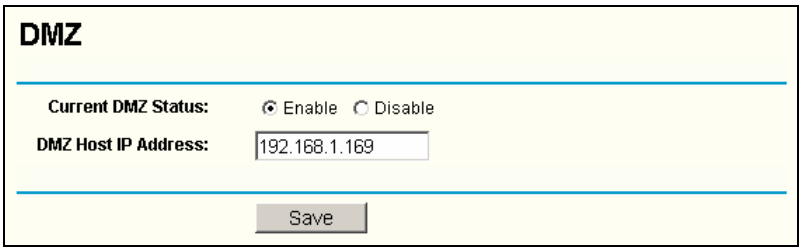


Figure A-6 DMZ

4. I want to build a WEB Server on the LAN, what should I do?

1) Because the WEB Server port 80 will interfere with the WEB management port 80 on the router, you must change the WEB management port number to avoid interference.

2) To change the WEB management port number: Login to the router, click the "Security" menu on the left of your browser, and click "Remote Management" submenu. On the "Remote Management" page, type a port number except 80, such as 88, into the "Web Management Port" field. Click "Save" and reboot the router.

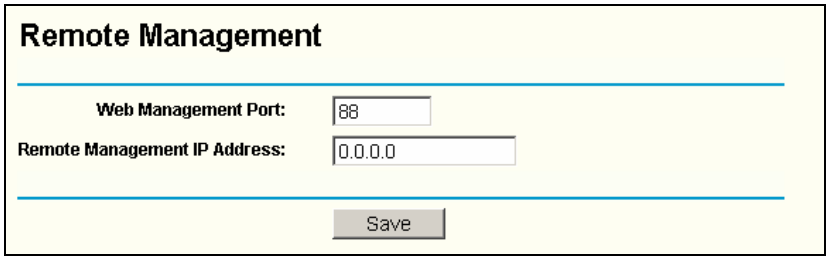


Figure A-7 Remote Management

Note: If the above configuration takes effect, to configure to the router by typing http://192.168.1.1:88 (the router's LAN IP address: Web Management Port) in the address field of the web browser.

3) Login to the router, click the "Forwarding" menu on the left of your browser, and click the "Virtual Servers" submenu. On the "Virtual Server" page, enter "80" into the blank below the "Service Port", and your IP address below the IP Address, assuming 192.168.1.188 for an example, remember to "Enable" and "Save".

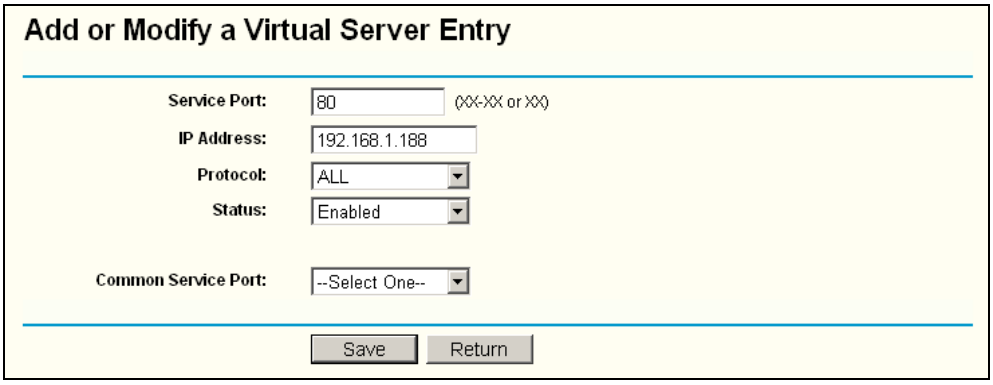


Figure A-8 Virtual Server

Appendix B: Configuring the PCs

In this section, we'll introduce how to install and configure the TCP/IP correctly in Windows XP. First make sure your Ethernet Adapter is working, refer to the adapter's manual if needed.

1. Install TCP/IP component

1) On the Windows taskbar, click the **Start** button, point to **Settings**, and then click **Control Panel**.
2) Click the **Network and Internet Connections** icon, and then click on the **Network Connections** tab in the appearing window.
3) Right click the icon that showed below, select Properties on the prompt page.

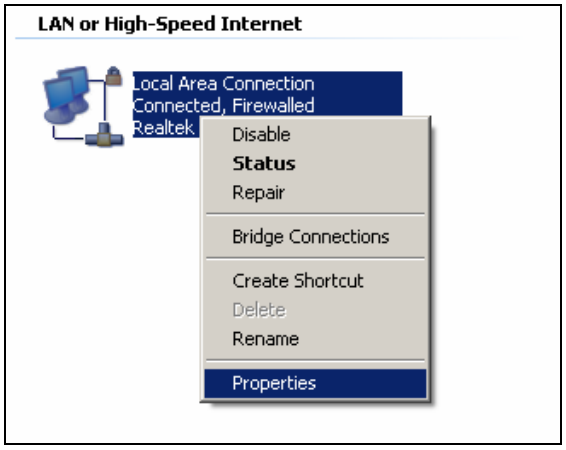


Figure B-53

4) In the prompt page that showed below, double click on the **Internet Protocol (TCP/IP)**.

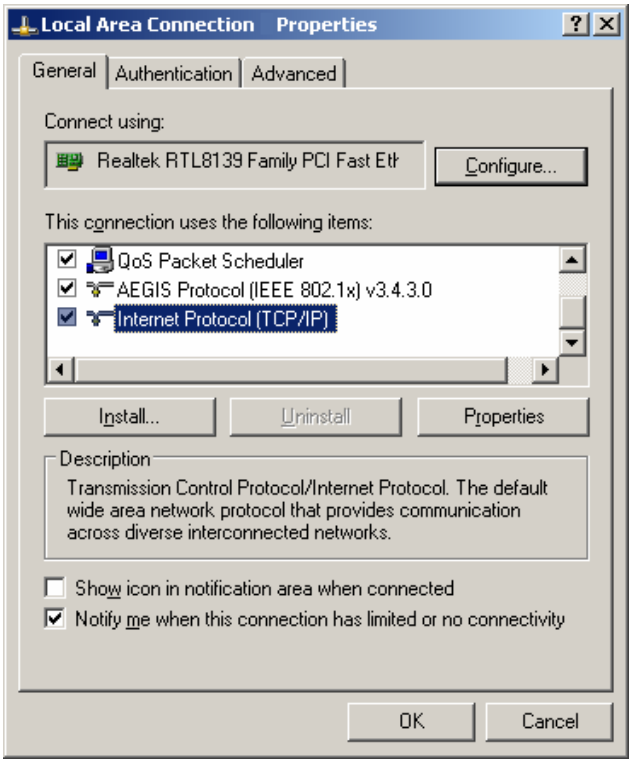


Figure B-54

5) The following **TCP/IP Properties** window will display and the **IP Address** tab is open on this window by default.

Now you have two ways to configure the **TCP/IP** protocol below:

➢ **Setting IP address automatically**

Select **Obtain an IP address automatically**, Choose **Obtain DNS server automatically**, as shown in the Figure below:

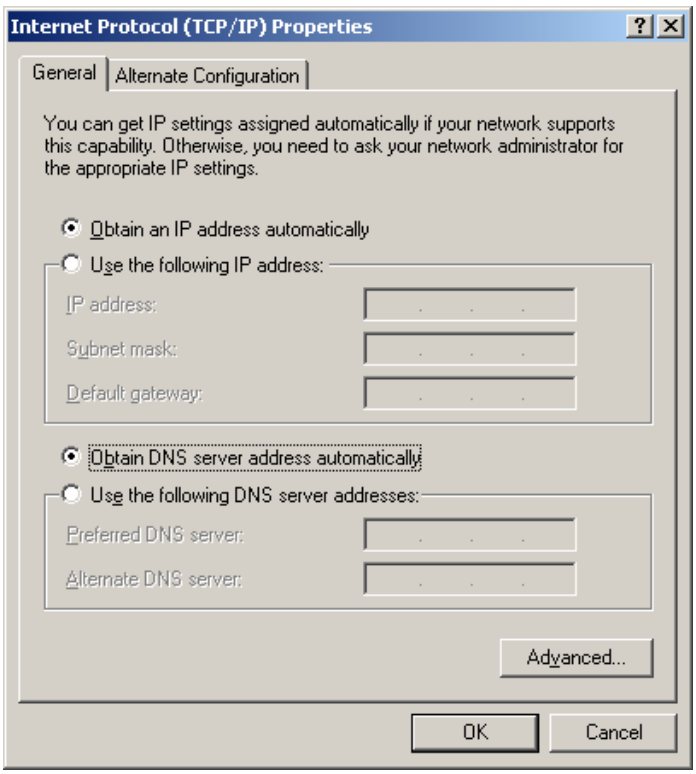

Internet Protocol (TCP/IP) Properties
General
Alternate Configuration
You can get IP settings assigned automatically if your network supports this capability. Otherwise, you need to ask your network administrator for the appropriate IP settings.
Obtain an IP address automatically
Use the following IP address:
IP address:
Subnet mask:
Default gateway:
Obtain DNS server address automatically
Use the following DNS server addresses:
Preferred DNS server:
Alternate DNS server:
Advanced...
OK
Cancel

Figure B-55

➢ **Setting IP address manually**

1 Select **Use the following IP address** radio button. And the following items available

2 If the router's LAN IP address is 192.168.1.1, type IP address is 192.168.1.x (x is from 2 to 254), and **Subnet mask** is 255.255.255.0.

3 Type the router's LAN IP address (the default IP is 192.168.1.1) into the **Default gateway** field.

4 Select **Use the following DNS server addresses** radio button. In the **Preferred DNS Server** field you can type the DNS server IP address, which has been provided by your ISP

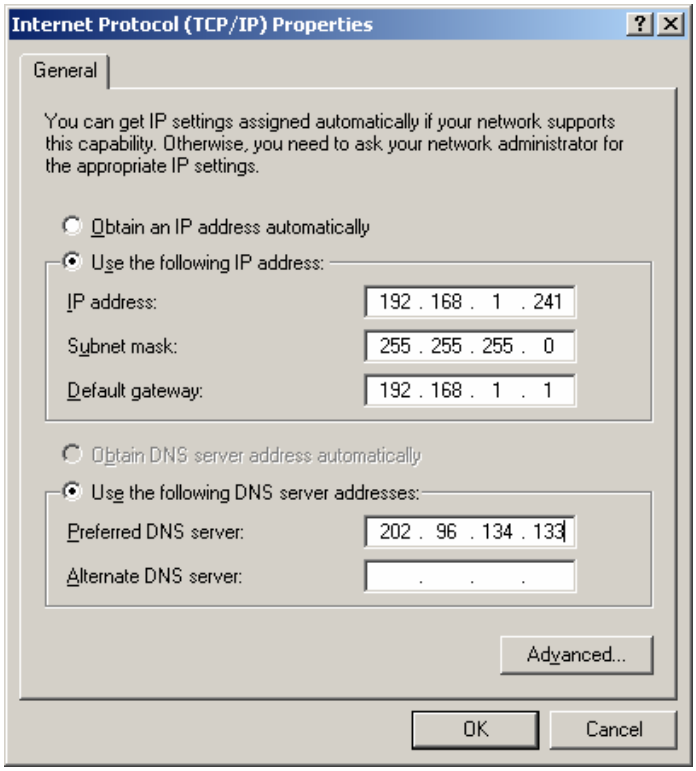

Internet Protocol (TCP/IP) Properties
General
You can get IP settings assigned automatically if your network supports this capability. Otherwise, you need to ask your network administrator for the appropriate IP settings.
Obtain an IP address automatically
Use the following IP address:
IP address: 192 . 168 . 1 . 241
Subnet mask: 255 . 255 . 255 . 0
Default gateway: 192 . 168 . 1 . 1
Obtain DNS server address automatically
Use the following DNS server addresses:
Preferred DNS server: 202 . 96 . 134 . 133
Alternate DNS server:
Advanced...
OK
Cancel

Figure B-4

Now:

All the configurations are finished; it will take effect after reboot your computer.

Appendix C: Specifications

General	
Standards	IEEE 802.3, 802.3u
Protocols	TCP/IP, PPPoE, DHCP, ICMP, NAT, SNTP
Ports	One 10/100M Auto-Negotiation WAN RJ45 port. Eight 10/100M Auto-Negotiation LAN RJ45 ports supporting Auto MDI/MDIX
Cabling Type	10BASE-T: UTP category 3, 4, 5 cable (maximum 100m) EIA/TIA-568 100Ω STP (maximum 100m) 100BASE-TX: UTP category 5, 5e cable (maximum 100m) EIA/TIA-568 100Ω STP (maximum 100m)
Power Supply	9V~ 0.8A
LEDs	Power, System, Link/Act
Safety & Emissions	FCC, CE

Environmental and Physical	
Operating Temp.	0℃~40℃ (32℉~104℉)
Operating Humidity	10% - 90% RH, Non-condensing
Dimensions (W x D x H)	7.9 x 5.5 x 1.1 (inch)

Appendix D: Glossary

- **DDNS** (**D**ynamic **D**omain **N**ame **S**ystem) **-** The capability of assigning a fixed host and domain name to a dynamic Internet IP address.
- **DHCP** (**D**ynamic **H**ost **C**onfiguration **P**rotocol) **-** A protocol that automatically configure the TCP/IP parameters for the all the PCs that are connected to a DHCP server.
- **DMZ** (**D**e**m**ilitarized **Z**one) **-** A Demilitarized Zone allows one local host to be exposed to the Internet for a special-purpose service such as Internet gaming or videoconferencing.
- **DNS** (**D**omain **N**ame **S**erver) **-** An Internet Server that translates the names of websites into IP addresses.
- **Domain Name -** A descriptive name for an address or group of addresses on the Internet.
- **DoS** (**D**enial **o**f **S**ervice) **-** A hacker attack designed to prevent your computer or network from operating or communicating.
- **DSL** (**D**igital **S**ubscriber **L**ine) **-** A technology that allows data to be sent or received over existing traditional phone lines.
- **ISP** (**I**nternet **S**ervice **P**rovider) **-** A company that provides access to the Internet
- **MTU** (**Maximum Transmission Unit**) **-** The size in bytes of the largest packet that can be transmitted.
- **NAT** (**N**etwork **A**ddress **T**ranslation) **-** NAT technology translates IP addresses of a local area network to a different IP address for the Internet.
- **PPPoE** (**P**oint to **P**oint **P**rotocol **o**ver **E**thernet) **-** PPPoE is a protocol for connecting remote hosts to the Internet over an always-on connection by simulating a dial-up connection.

Appendix E: Contact Information

For help with the installation or operation of the TP-LINK TL-R860 Cable/DSL Router, please contact us.

Website: http://www.tp-link.com